

## مقدمة عن الشبكات

## Introduction To Network

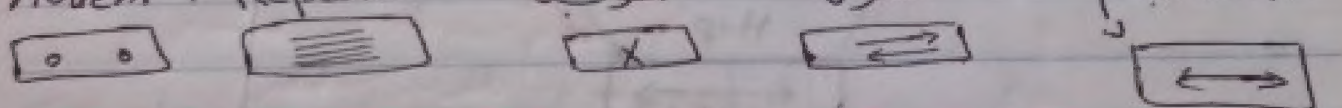
### ما هي الشبكة؟

Network is a group of computers connected with other to share data.

هي مجموعة من الحواسيب متصلة مع بعضها لتشاركة البيانات

### Network Components

### مكونات الشبكة

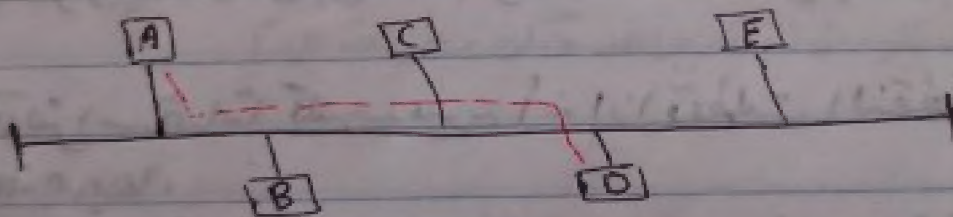
1. PC's أجهزة الكمبيوتر
2. Cables الكابلات
3. Network devices : Router - Switch - NIC, Hub -  
Modem & Repeater الموجه المحول (تأثير شبكة)   


### Network Topologies

### بنية أو طريقة الشبكات

#### ① Bus Topology

#### ① الشبكة الخطية



من هذه الطريقة إذا كان A يرسل إلى D البيانات تصل إلى جميع الأجهزة C & B & E وأيضا عكس وهو half duplex

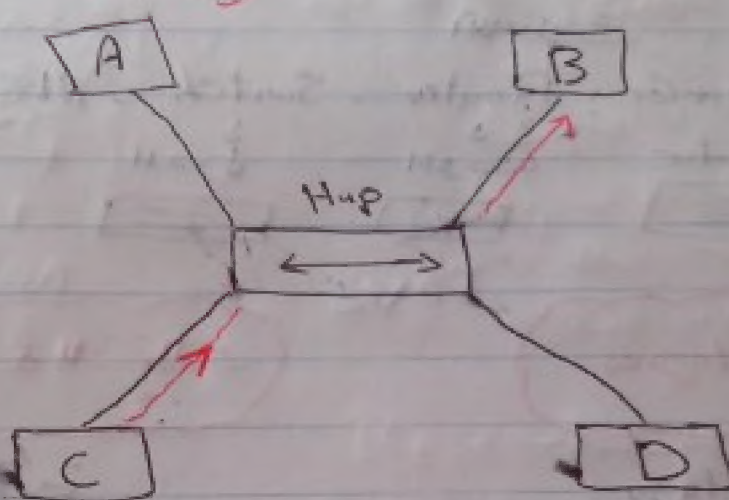
وهو أنه تكون هناك قناة واحدة للرسالة والاستقبال ومثال على ذلك أجهزة اللاسلكي من استخدام رجال الشرطة لها فالطرف الأول يتكلم ثم يقول [حول] حتى يعلم الطرف الثاني أنه انتهى منه الكلام فيستطيع الطرف الثاني



أن يتكلم عن الطرف الأول أن يتكلم له وهكذا.  
 ومن عيوب هذا النوع أيضًا أنه إذا كان A يرسل إلى B فلا يستطيع  
 C أن يرسل إلى D إلا بعد انتهاء عملية النقل بين A و B  
 - أمثلة على هذا النوع من الشبكة  
 (الشبكات المركزية) فمماثلة شبكة يرسل من أحد الأطراف بيانات إلى  
 الأطراف الأخرى التي تستقبل البيانات.

## [2] Star Topology

[2] شكل الشبكة



تكونه من نقطة مركزية متصل بكل الأجهزة ليتكون من الشبكة  
 (Star)

هذا النوع هو الأكثر استخدامًا لأنه من عيوبه أنه إذا قطعت النقطة المركزية  
 تسقط الشبكة بأكملها.

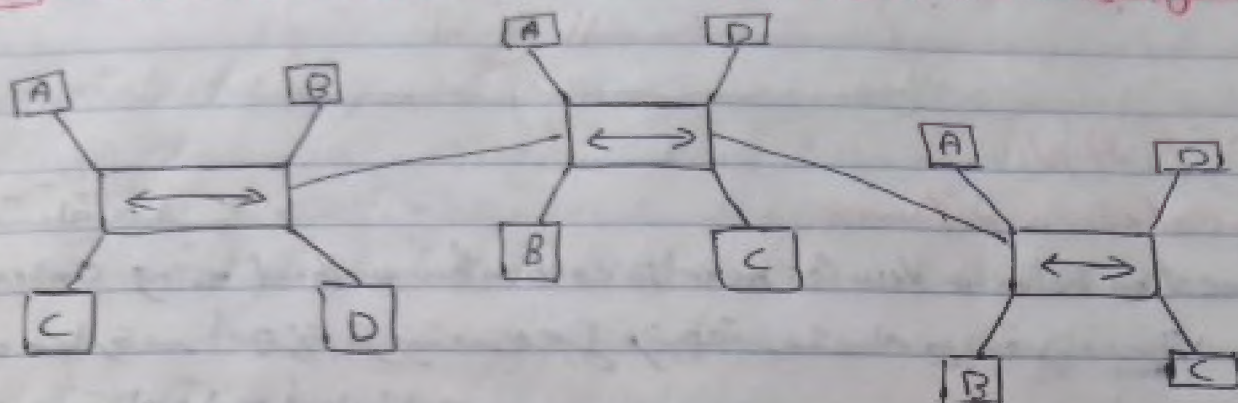
في هذه الشبكة النقطة المركزية تستقبل البيانات من العرف C مثلاً ثم توجه  
 البيانات إلى الطرف B كما في الصورة.

**★ Transmission through a central point.**



### [3] extended star

شكل النجمة المتشعبة أو الممتدة

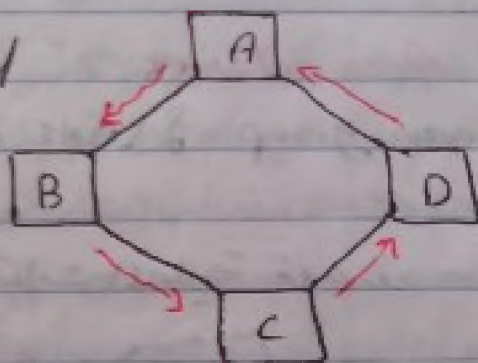


هو نفس فكرة star topology لكنه بصورة متشعبة وممتدة.  
# More resilient than star topology أكثر مرونة من نجمة أو بولج

### [4] Token Ring Topology

شكل الحلقة أو الدائرة

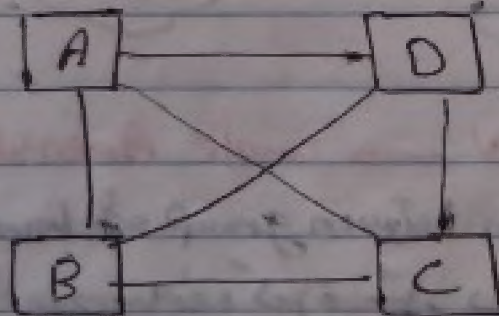
Signals travel around ring



طريقة توصيلها تكون على شكل حلقة أو من أضياع وهو Half duplex  
الارسال يكون من اتجاه واحد وتكون ببطء جداً

### [5] Mesh Topology

جميع الاطراف متصلة ببعض البعض  
عبر كل سرعة السائل ومكلفة  
التنفيذ أو الشبكية



Highly Fault-tolerant  
Expensive to implement



# Network Types انواع الشبكات

## ① LAN

Local Area Network

شبكة محلية .  
Connection between devices near to each other without using central office.

هو عبارة عن أجهزة قريبة من بعض من نقطة ومتمصلة مع بعض دون الحاجة إلى خزان مركزي أو ممتد به

غالباً تكون في حدود الـ 10 كيلومتر وبعض أدمه هي الشبكة التي تغطي

انشاءات الشركة الاستفاداة من أحد طرفي آخر مثل (ISP) internet service provider  
وهي شبكات المزودة لخدمة الانترنت مثل Te Data - link.

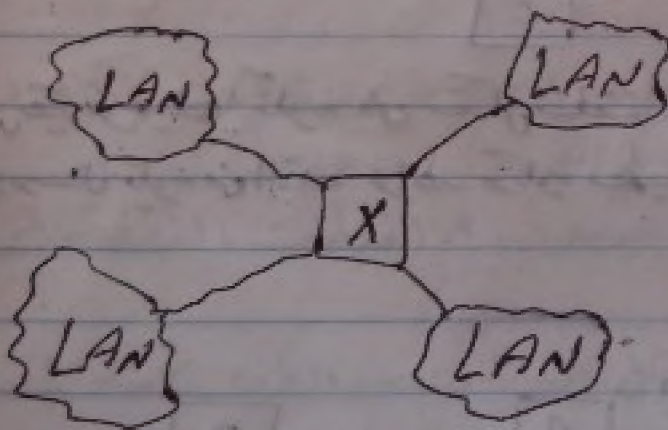
## ② Man

Metropolitan Area network

شبكة مدينة أو العاصمة

Connection between group of LANs over a small area within city like Cairo.

هو اتصال بين مجموعة من الشبكات المحلية في حدود مدينة مثل القاهرة  
تستخدم فيها شركات ISP



## ③ WAN → wide Area Network

شبكة المنطقة الواسعة

Connection between group of LANs over a large Area like countries

اتصال بين مجموعة من الشبكات المحلية في حدود مناطق كبيرة مثل دولة ودولة أخرى



## How Data Transfers

دراسة كل علم وله قواعد يبنى عليها هذا العلم فعلم الرياضيات مثلاً يبنى على الجمع والطرح والقسمة والضرب فلا يصح الدارس دراسة التفاضل والتكامل من باب المثلثات مثلاً من غير دراسة الجمع والطرح والقسمة والضرب لذلك علم الشبكات يبنى على 7 طبقات (7 layer) ستقوم الآن بدراسة كل بصورة مختصرة قبل التلخيص بالتفصيل

## OSI model "open System InterConnection"

بداية عملية نقل البيانات تمر بسبع مراحل أو طبقات في هذا النموذج وهي التي تظهر في الرسم

PC ①

PC ②

Application	كل ما يتعلق بالبيانات من الجهاز	Application
presentation	① إلى الجهاز رقمي في قمر البيانات	presentation
Session	المختلفة من الجهاز فهو واحد متر	Session
Transport	تجربة Application presentation	Transport
Network	② Session . . . physical	Network
Data link	ثم يتجهل الجهاز ③ البيانات ومقر	Data link
physical	أخيراً ينفذ الطبقات كلها العكس	physical
Application up Data link physical		

## ① Application layer

why a layered network model?

- ① Reduces Complexity . تقليل التعقيد
- ② Simplifies teaching and learning . تسهيل التعليم والتعلم



### ① Application Layer

used to represent a user interface to the network

بإختصار، البرامج التي يتفاعل معها المستخدم مثل Browsing، yahoo msg.

### ② presentation Layer

- Ensures that Data is Readable by receiving system تأكد من إمكانية القراءة
- Formats Data تنسيق البيانات
- Structure Data هيكلية البيانات
- Provides encryption تقوم بعملية التشفير

بإختصار، هذا نفس طبقة Application لكنه presentation هو البيانات كيف نرى تراها على الكمبيوتر فمثلاً فيلم على جهاز ما يقرأ كالتالي  
فيلم... أنا عليه تشفير للبيانات أما أنا الفيلم يراه الشخص بصورة  
فيلم بينما يراه الجهاز نفسه كما رقماً.

### ③ Session Layer

- Interhost Communication تفتح قناة اتصال
  - Give order for: establishment of session  
management of session  
Termination of session between source and destination.
- ← إنشاء  
← إدارة  
← إنهاء

Session قد تكون تفتح أو تميل

### ④ Transport Layer

من هذه الطبقة يتم تقسيم البيانات إلى أجزاء "Segment"  
ويتم تسمية البيانات هذه الطبقة إلى "Segment".  
من هذه الطبقة أيضاً يتم استخدام نوع من النقل



Transmission Control Protocol

TCP



reliable service

Sequenced

~~Secure~~

Connection oriented

Virtual Circuit

ACK "acknowledgment"

User Datagram Protocol

UDP



unreliable service

unsequenced

~~unsecure~~

Connection less

No ACK

### شرح الفرق بين TCP/UDP

بافتتاح كلاهما برؤوس نقل للبيانات كل منهما لها مميزات وأما هو:

1- TCP يضمن وصول البيانات بشكل سليم فيه أنه ذلك غير مضمون

UDP

2- TCP يرسل البيانات بشكل متسلسل مرتب فيه لا يرسل UDP بشكل متسلسل أو مرتب

3- TCP يثبث اتصال موجه إذا اتصال مباشر أو غير مباشر دائرة ظاهرية فيه المرسل والمستقبل بينما لا يقدم UDP هذه الخدمة

4- TCP فيه يرسل Segments نقل Segments مكونه من شكل تسلسل ويتم انتظامه بالتسليم إذا لم يتقبل منه الطرف الآخر ينادى عليه يتم إرسال

ال Segment التالي وإذا لم يتقبل ACK فليس يتم إرسال ال Segment التالي أما UDP فيتم إرسال ال Sequence دون انتظار أو التأكد من الاستقبال السليم لها

5- TCP أيضاً فيه UDP ليس عليه التحقق والتوثيق المتعينه عنه UDP

6- في أوضاع الأمثلة TCP ← email بينما أوضاع الإثبات UDP هو البث المباشر

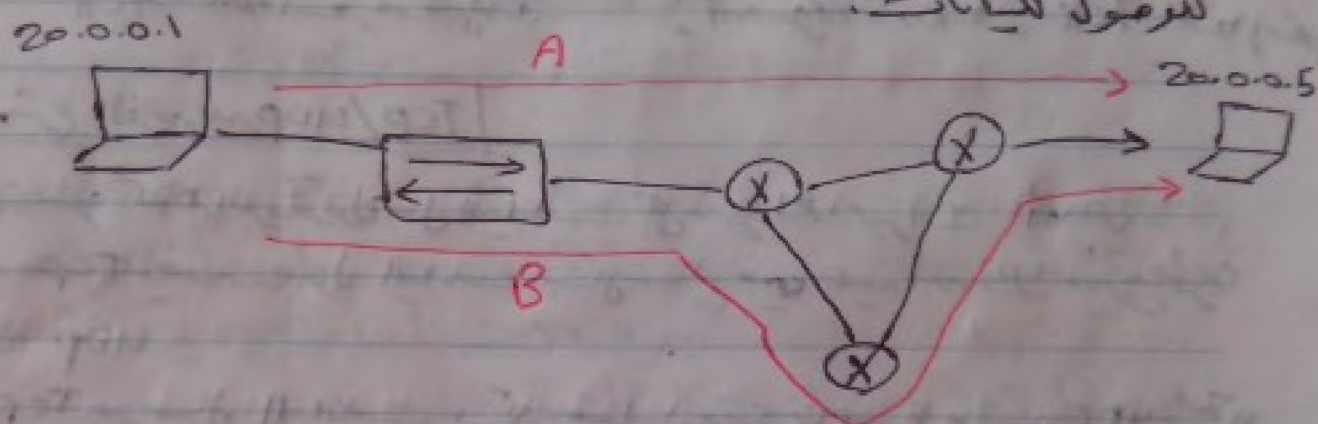


## ⑤ Network Layer

من هذه الطبقة يتم تسمية النطاق packets وفي هذه الطبقة يتم استخدام الراوتر الذي وظيفته توجيه واختيار أفضل طريق لنقل البيانات وإيضاح هذه الطبقة يتم إنشاء عنوان المصدر Source IP وعنوان الوجهة des. IP

مثال

بفرض أن هناك جهاز هو Source IP رقمه أو عنوانه 20.0.0.1 يرسل بيانات إلى des IP رقمه 20.0.0.5 كما بالرسم يظهر أكثر من طريق للوصول للبيانات.



من هذه الحالة يعرف الراوتر (X) باختبار أفضل الطرق وهو الطريق A حيث أنه به عدد أقل من الراوترات والتوصيلات من الطريق B فيظهر لنا في المثال بعد الراوتر وهو اختبار أفضل الطرق.

## الخلاصة لـ Network layer

- ① Routes Data packets توجيه حزمة البيانات
- ② Selects best path to deliver data اختيار أفضل الطرق للتوصيل
- ③ Provides logical addressing. إنشاء عنوان منطقي، إرسال أولافانة إلى المستقبل النهائي

## ⑥ Data link layer

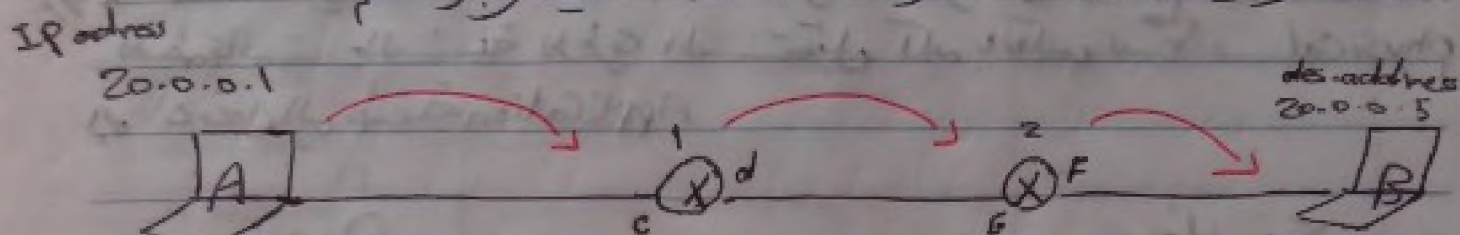
من هذه الطبقة يتم إضافة mac address وهو اختبار كلمة media access control ويسمى أيضا physical address أي العنوان الحقيقي وهو مختلف عن IP address في طبقة Network فهو عنوان logical وهمي



مال mac address بإختصار عنوان كرت اى Lan أو رقم كرت اى Lan  
الذي يميزه به غيره من جميع الكروت الموجودة في العالم عادة يتكون من 12 رقم وهرق  
وتنقسم إلى 6 أرقام هذه هي الصورة Frame

مثال

نفسه ان هناك جهاز A يرسل داتا الى الجهاز B وكانه Ip address هو  
20.0.0.1 وال des address هو 20.0.0.5 كما يظهر بالرسم



ففيه يتم نقل البيانات لا يتغير كل من Ip address ولا حتى des address فيه  
أن ال mac address يتغير فعند إرسال الداتا من الجهاز A إلى الراوتر  
الاول يكون ال source mac address هو رقم الجهاز A ويكون des mac address  
هو المدخل E من الراوتر الاول ثم تخرج الداتا من الراوتر الاول فتكونه src mac address  
هو المخرج d وتكونه des mac address هو المدخل E ثم تخرج الداتا من الراوتر  
الثاني من F وهو src mac address إلى des mac address وهو الجهاز B  
تفهم من ذلك أن Ip address لا يتغير في حينه يتغير  
mac address كذا خرج الداتا من الجهاز A وعبرها على الراوتر حيث أن  
الراوتر به كارت Lan مثل جهاز الكمبيوتر تماماً

هذه العملية التي نضيف فيها عنوان المالك إلى ال Frame وإزالته  
من كل مرة يمر الراوتر من جهاز لتسمى encapsulation وتغليف و  
تغليف التغليف أي يتم إضافة عنوان المالك عند الانتقال من الجهاز للراوتر الاول  
ثم تخرج الداتا من الراوتر الاول وتكونه src mac address للراوتر الثاني ثم  
عملية جديدة من encapsulation التغليف ثم لنقل الداتا من الراوتر الثاني إلى  
من الراوتر الثاني إلى الجهاز B يتم إضافة encapsulation

الخلاصة

- ① Hop to Hop Data delivery.
- ② mac addressing
- ③ Hop to Hop error detection.
- ④ Formatting Data.



## ② physical Layer

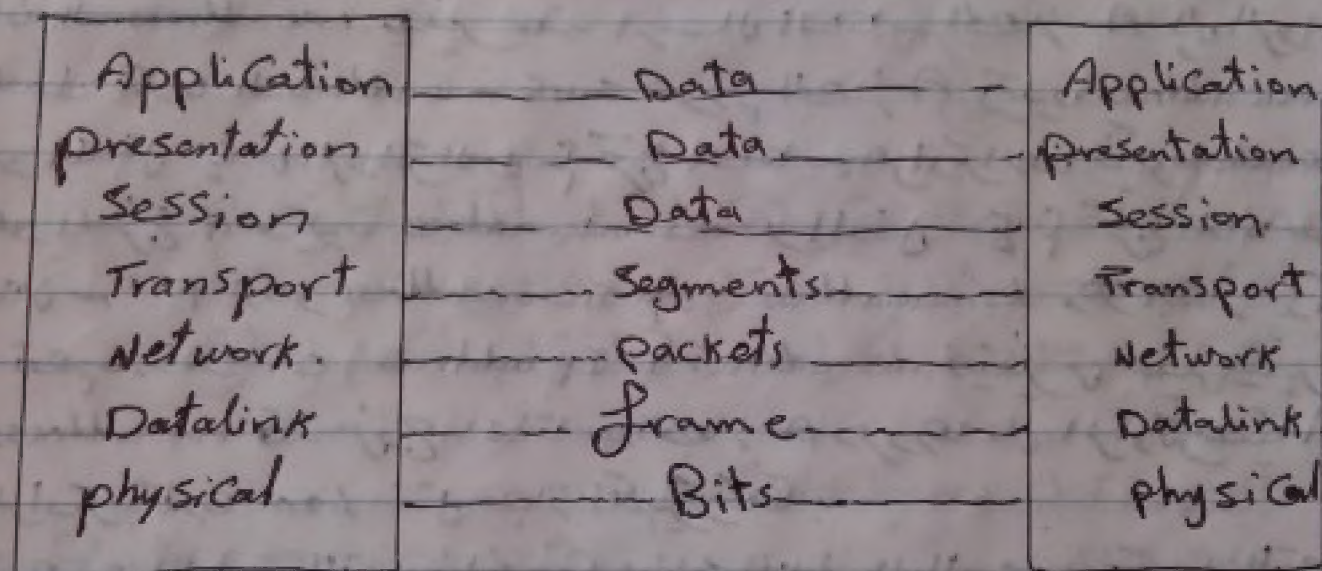
في هذه المرحلة أذا الطبقة تم تحويل ال frame إلى Bits في كبرياء  
وهذا الطبقة المسؤولة عن جميع المعدات المعلقة للشبكة على أنواع الكابلات وكما سيعمل  
تحويل البيانات لكونه ككبرياء

\* هنا ينتهي العمل من جانب الطرف المرسل ويتم نفس الوظائف  
للطبقات بالنسبة للطرف المستقبل لكنه بالعكس تبدأ ال physical  
أي أن نقل ال طبقة Application

Sender



Receiver



# هنا #

العملية التي تربط البيانات من الجانب المرسل بداية من طبقة  
Application إلى physical تدعى عملية encapsulation

العملية التي تربط البيانات من الجانب المستقبل بداية من طبقة physical  
إلى Application تدعى عملية decapsulation



## Top/Ip Protocol suite / model

استخدمه مزيج وزارة الدفاع الأمريكية لتكون مع 7 طبقات



\* يوجد Top/Ip أكثر انتشاراً من OSI في العالم

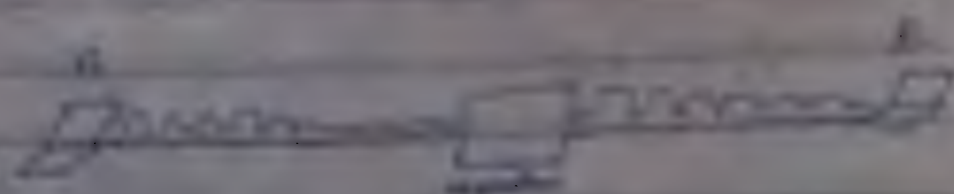
- ① Flexible addressing scheme ② مرن في معالجة العنوان
- ② usability by most operating systems and platforms.
- ③ لا يلزم استخدام كل طبقاته أثناء الاتصال بالإنترنت
- ④ The need to use it to connect to the internet.

## Network Devices

### ① Layer 1 devices

في الطبقة الأولى من نموذج TCP/IP، الأجهزة التي تعمل على مستوى الطبقة الأولى

### ① Repeater

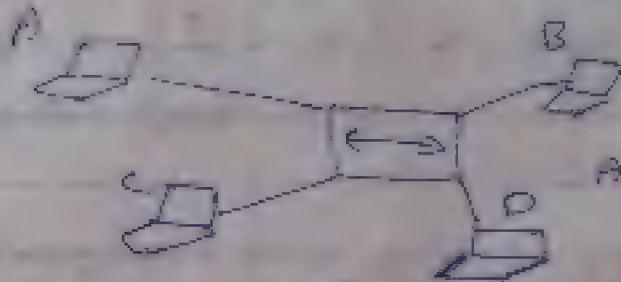




ووظيفته ان يجمع بين عدة شبكات ويوصلها ببعضها البعض  
 يكون حاسباتها حاسبات متصلة ببعضها البعض

## ② Hap

تعبارة عن Repeater متعدد المنافذ multi port repeater



طريقة عمل Hap يمرر الإشارة أيضاً

ويكرر كل ما يراه عينا كبر وهو عند ما يرسل A

وإذا كان B فلا حاجة ان Hap لا يعرف B

لأنه لا يعرف ذلك يقوم بإرسال الإشارة لكل الأجهزة على الشبكة مما يؤدي إلى صنف مالمس Loop  
 وهو انه يكرر البيانات التي تم استقبالها من الأجهزة مما يؤدي إلى تشكيل الشبكة وحفظ

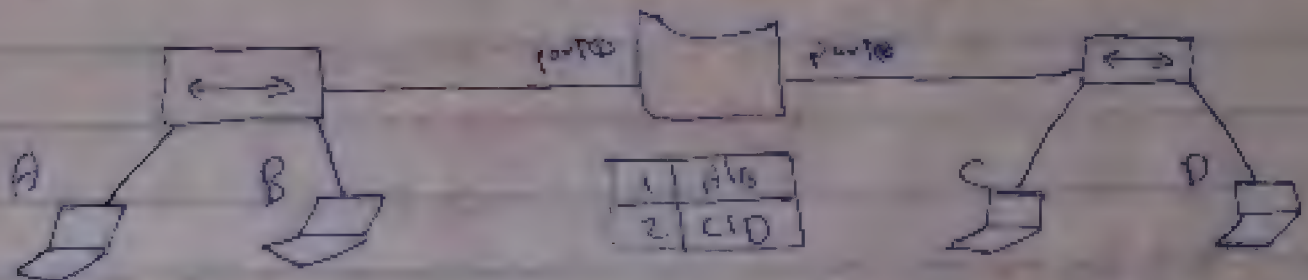
## ② Layer 2 Devices

هي الأجهزة التي تعمل في الطبقة الثانية "Data link layer"

① NIC "Network Interface Card" كارت الشبكة

## ② Bridge

Bridge تسمى جسر وتضع طريقة عمله في الشكل



إذا كان A يرسل إشارة إلى B فلا حاجة ان Bridge لا يمرر الإشارة إلى الأجهزة

على البورت 1 وهذا C/D وكذلك إذا كان C يرسل إشارة إلى D فإنه لا يمرر

الإشارة إلى الأجهزة على البورت 2 A/B. تلكه إذا أرسل A إلى D فإنه

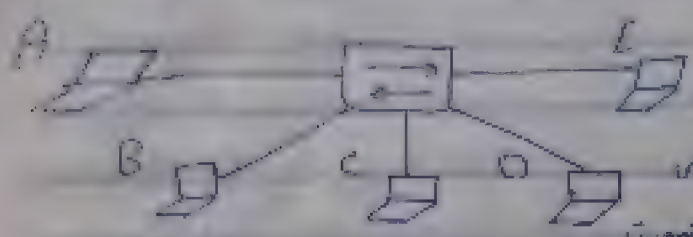
Bridge يقوم بتقسيم الإشارة إلى البورت 2 للوجهات C و D فقط كما يصل

إلى الوجهات المراد D أي أنه السوالب Bridge يقلل من Loop ويمنع حدوث Hub



### [3] Switch

يُعتبر بديلًا عن مرسلة البيانات Bridge التي تعمل على مستوى الطبقة الثانية من النموذج وتقوم بتمرير الحزم من المحطات.



- إذا قام A بمرسل بيانات الجهاز E فتكون  
خارجة المرسلة فتقوم بإرسال الحزم (Frame) إلى  
الجهاز E لأننا الجاهزة لا يعرفها الجهاز E على البورت

نقوم بمرسل إلى Frame إلى كل الأجهزة كما يفعل ال Hub لكنه ما عني أنه  
يسجل ال mac address الخاص بكل جهاز والبورت الخاص به في جدول يسمى Cam table  
أوليس أيضا mac address table فعند بداية تشغيل ال Switch يكون هذا الجدول فارغ  
فعند إرسال أحد Frame يسجل ال mac الخاص بال PC أو سورس وهو الجهاز A  
من المثال و يرسل ال Frame لكل الأجهزة ويبدو فقط الجهاز A في المثال  
في سجل ال mac الخاص به كما أن بورت ال Switch وحدها من قبل الحزم إلى ال A لأنه لنقل  
الحزم لديه مخصص لو أرسل ال A إلى D مثلا تخرج البيانات من ال A إلى D فقط  
وبالتالي يقلل حدوث ال Loop

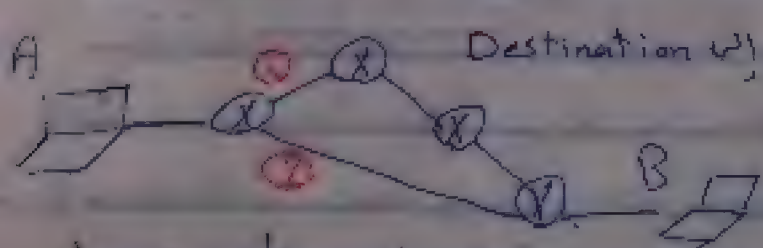
A	port 1		
B	port 2	D	port 4
C	port 3	E	port 5

وخرصة نقل الحزم  
الجدول يسجل به ال mac الخاص بالمرسل والمستقبل في  
كل عملية أي أنه يملك الجدول عندنا لا يتم إرسال البيانات  
لكن أطراف الشبكة لكنه عند إرساله فقط لأنه تم تسجيل المخرج الذي يجب أنه  
تخرج البيانات للوصول للجهاز المطلوب

### [3] Layer 3 Devices

هي الأجهزة التي تتقدم من الطبقة الثالثة "Network layer"

#### Router (X)

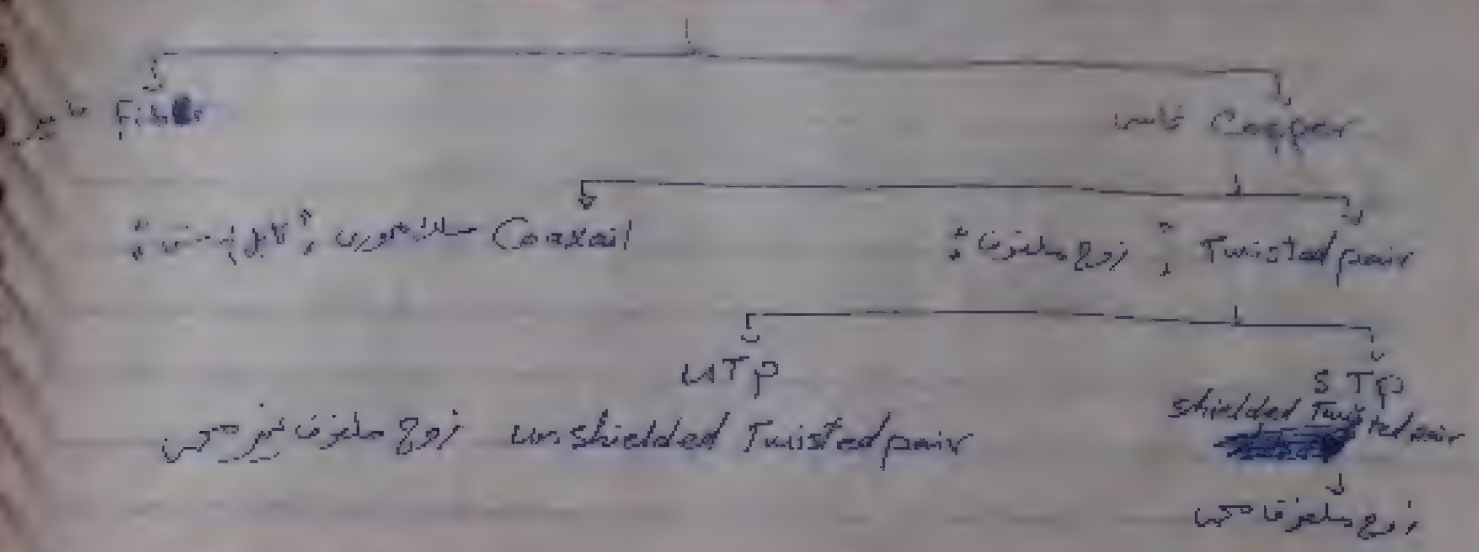


يقوم الراوتر باختيار أفضل مسار للوصول إلى Destination  
يتفقد في المثال نلاحظ

في المثال يظهر أنه أفضل طريقة ليكن الوصول به إلى  
الجهاز B هو الطريقة الثانية فيقوم الراوتر بنقل البيانات من خلال  
يسجل ال Routing Table ثم يسهل تسجيل كل جهاز وأيضًا روابط الموصلة اليه



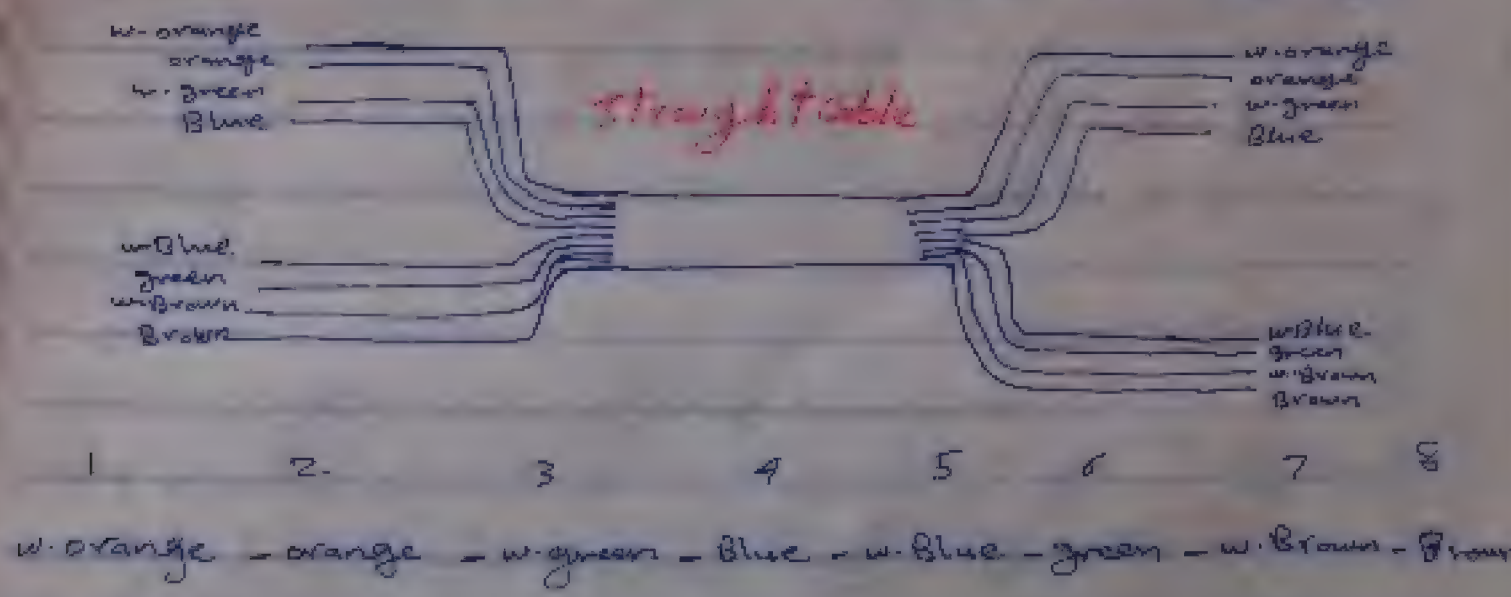
# The Cables



طريقة التوصيلات بوضع ذلك في الجدول

1	2
pc Router	Hub Switch

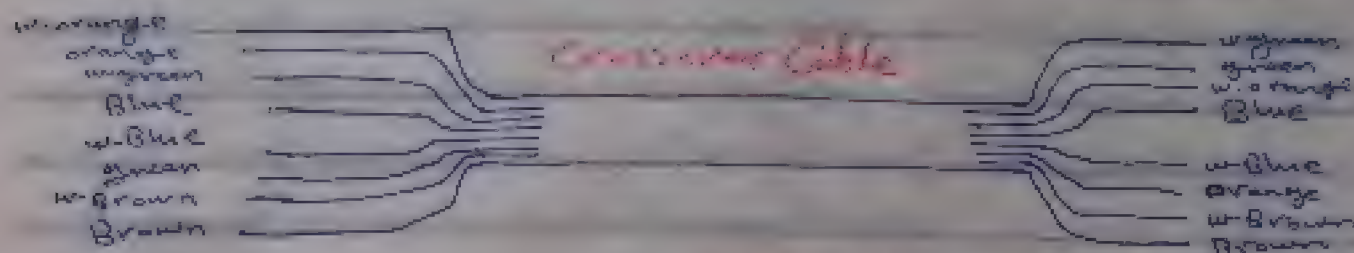
① اذا وصلنا أي جهاز من النوع ① بأى جهاز من النوع ② نستخدم وصلة straight  
 ② اذا وصلنا أي جهاز من النوع ① بجهاز من نفس النوع ② بجهاز من نفس النوع  
 تكون الوصلة اسودا Crossover





## ثلاث حزم

فردية البرصية يكون لها الطول نفسه سواء كان Straight أو ملتوي. والطول الآخر يتم استيعابه في اللون الأبيض البهري. والبرصية البهريّة لها الطول نفسه والآخر يتم استيعابه في اللون الأبيض البهري. ٦ حزم و ٣ حزم



Straight يكون طرف من طرف واحد

والطرف الآخر يكون بترتيب آخر كما يلي

3 6 1 4 5 2 7 8

w. green - green - w. orange - Blue - w. Blue - ~~orange~~ - w. Brown - Brown

Cat 5 - أربعة أزواج

Cat 5e - أربعة أزواج

Cat 6 - ستة أزواج

تصنيفات

ثلاث Twisted pair

Twisted pair

Base T - أربعة أزواج

Fast Ethernet Cat 5e

Cat 5 - Ethernet

Gig Ethernet - Cat 6

Repeater - أجهزة التكرار التي تربط بين الشبكات المحلية وتحتل



## Switching

السويتش من الأجهزة التي يتم التعامل معها مبرمجيا فالعامل في السويتش يكون  
الآنزومس التعامل مع البروتوكول

السويتش يتعامل مع mac address وهو اختصار Media Access Control  
وهو رقم كرت الشبكة وهو رقم ثابت لا يستطيع تغييره ولا يشابه مع الرقم للكرت  
شبكة آخر وهو رقم سلسل عتري  $hexadecimal$  يتكون من الارقام (0-9) و  
حرف (A-F) والمات يكون من 48 bits.

السويتش هو Layer 2 Device لأنه لا يفهم ال IP ولكنه يفهم ال Layer 2  
للوصول على رقم ال mac address من قبله الامر  
يظهر لنا اسم المات وتكون ال physical address وتكون من 17 رقم  
معرفة

ال mac address لديه أنه يشابه مع رقم كرت آخر ولا يستطيع تغييره وبالتالي  
عند توصيل أجهزة الكمبيوتر بالسويتش يتواصل معها ويرى المات الخاص بكل  
جهاز عن طريقه بروتوكول ARP

## ARP protocol

بروتوكول ARP هو اختصار Address Resolution Protocol وظيفته هو ان يواصل  
مع جهاز الكمبيوتر يعرف ال mac address الخاص به ويحمله في switching table  
الخاص بالسويتش وال switching table هو الذي يحين السويتش عن ال Hub  
فال Hub لا يعرف ال mac address وبالتالي يرسل المات لكل الأجهزة ما يوجد في حوض  
حاسوب Loop كليه السويتش ليحفظ المات الخاص بكل جهاز في switching table  
ويقوم بجلبه لتسهيل معرفة المات بروتوكول ARP وبالتالي يرسل المات يرسل  
السويتش من Source إلى ال Destination ولا يتم إرسال المات لكل الأجهزة



\* عند توصيل الموجهات بالكمبيوتر يتم توصيل الموجهات مباشرة بجهاز الكمبيوتر  
من خلال الـ 24 ثنائي من بورتات الموجه

- ① Listening ← مرحلة الموجه يبحث فيها عن العناوين المخصصة
- ② Learning ← مرحلة الموجه يبحث فيها عن تسجيل الـ mac address
- بعد المرحلة لنقل في المرحلة الـ Forward وهو مرحلة الإرسال والاستقبال

\* يتكون الموجهات غالباً من 24 بورت تنقسم هذه البورتات إلى قسمين أحدهما توصيل الموجهات

- مضاتك خارجة تكون ← ethernet ← 10 ميجا / ثانية
- مضاتك خارجة ← Fast ethernet ← 100 ميجا / ثانية
- مضاتك خارجة ← Gig ethernet ← 1 جيجا

## Switch Configuration

للتعرف على الأوامر التي سنستخدمها في عمل Configuration للموجهات لابد أن نعرف  
الـ modes الخاصة بالموجهات

### Switch mode

Switch > enable	User mode
Switch #	Privileged mode
Switch (config) #	Global Configuration mode
Switch (config-if) #	Interface mode
Switch (config-subif) #	Subinterface mode
Switch (config-line) #	Line mode

\* عند عمل إجراء الـ Configuration للموجهات يتم توصيل الموجهات بجهاز الكمبيوتر بواسطة Console  
مقبولة في الكمبيوتر بـ السيريل بورت ::: وبالـ الموجهات الخارجية ethernet



• لتفعيل السويتش وانتقال الى Privileged

Switch > enable or en

Switch #  $\longrightarrow$  privileged mode

• الانتقال من privileged الى Global Config.

Switch # Config T

Switch (config) #  $\longrightarrow$  global configuration

• الانتقال من Global Config الى Submode وكيه interface

Switch (config) # Interface Fa/  $\longrightarrow$  interface mode

Switch (config-if) #  $\longrightarrow$  subinterface mode

• للعودة من mode الى mode السابق نقوم Ctrl+Z أو edit

⑤ عند وضع استغراق [?] في mode يساعدك في معرفة الاوامر المتاحة في هذا المود

Switch > ?

Same Command for Switch

الآن سنتعرف على بعض الاوامر التي نستطيع من خلالها التحكم في السويتش

① تغيير اسم السويتش

Switch>en

Switch # Config T

Switch (config) # hostname Ahmed (or) host Ahmed



تحتل على جهازنا في كل وقت

و يمكن ان نستخدمه في كل وقت. الميزة التي توضحها هي اننا نستخدمه في كل وقت.

لذلك اننا نستخدمه في كل وقت. الميزة التي توضحها هي اننا نستخدمه في كل وقت.

Switch > en

Switch # Config T

Switch (config) # Line Console 0

Switch (config-line) # password 123 باسوردها 123

Switch (config-line) # login تفعيل الـ login

Switch (config-line) # exec-timeout 57 تجديد وقت تفعيل الـ login وبعدها يتوقف

وهو 5 دقائق ولا نحتاجه في كل وقت. (50) لا يتغير الـ password أبداً

(2) عمل الـ privileged mode

يتيح أيضاً التحكم في الـ privileged mode على الجهاز

Switch > en

Switch # Config T

Switch (config) # enable secret 123 باسوردها مشفرة

أو

Switch (config) # enable password 123 باسوردها غير مشفرة

ولكن الـ enable password 123 قبل المراجعة

Switch (config) # No enable secret (or) Switch (config) # No enable password

(3) التحكم في سرعة الـ Port

يمكننا أيضاً التحكم في سرعة البورت في الـ Ethernet

أو نستخدم الـ Fast Ethernet أو نستخدم الـ Giga Ethernet

حيث أنه كلما زادت السرعة بعد السرعة الفعلية للبورت



والتي تسمى سرعة البورت فيسواي

Switch > en

Switch # Config t

Switch(Config) # interface F0/1

Switch(Config-if) # Speed 10

Switch(Config-if) # Speed ?

ويقتصر لنا إما 10 ميجا / ثانية أو 100 ميجا / ثانية أو Auto وهو السرعة الافتراضية

البورت

Switch(Config-if) # Speed Auto

أداة السوفت التي تستخدم لإعداد

## ⑤ خاصية ال Full Duplex و خاصية ال Half Duplex

لفهم معنى ال Full Duplex وال Half Duplex لابد أن نفهم أنه كابل UTP مكون من 8 كابلات مبدآن الين والايضا الين كابل و يتقسم 4 كابلات وهي تستخدم في النقل ثلثه للتقدم فعليا يكون 2 كابلات وهذا انما هو خاصية ال Half Duplex وهذا عبارة عن أن ال هوسب يكون إما مستقبل أو مرسل لا يمكن أن يكون مرسل ومستقبل في نفس الوقت لأنه ذلك يؤدي إلى حدوث تصادم للبيانات Collision لذلك لم يتم استخدام بروتوكول CSMA/CD

## CSMA/CD protocol

بروتوكول ال CSMA/CD هو اختصار

Carrier Sense Multiple access / Collision Detection

يعمل هذا البروتوكول فقط في وضع ال Half Duplex وخصيسته عبارة عن منظم لعلية إرسال البيانات يقوم بعرضه على إرسال البيانات أولاً ثم يقوم بالسماح لها بالمرور في يتوقف على البيانات التي تتصلبه ومنع السماح لها بالمرور في الوقت الذي لا يكون فيه ذاتا أخرى مع إرسالها أو أنه يمنع عليه تصادم البيانات حيث لا يتم نقلها أو جزئياً لأن البيانات كانت ال Half Duplex فكل كابل واحد منظم البروتوكول بتنظيم عليه نقلها لمنع التصادم



في الواقع، كاستراتيجية Full  
هناك النوع يكون المقبول في حالة Half Duplex  
حيث أن النوع يكون مقبول في حالة Full Duplex  
في الواقع، لا ينبغي أن يكون CSMA/CD هنا النوع

Half Duplex vs Full Duplex impairment 7/7

Switch # Config T

Switch (config-if) # duplex half

### Duplex Full

Duplex Auto

منها حاله اذا تم تغيير وضع ال Duplex فـ السويتش الى وضع ال Full Duplex فانه كانت الشبكة المتصل به السويتش وانما هو جهاز الكمبيوتر يقول أيضا الى ال Full Duplex مباشرة فلهذا لا يتبع هذا برنامج ال Packet Tracer حيث لا يتبع ذلك بشكل او بآخر حيث يفترض ان تغيير تيارت الشبكة الخاص بجهاز الكمبيوتر من حاله ال Auto duplex الى حاله ال Depled

البان عبارة عن رسالة أو رسالة تحية إضافية للمسوقين أو مبيعات أو كترسالة ترحيبية  
أو كترسالة تحفيزية وينقسم البان إلى ثلاثة أقسام

Canter et al

مجلسنا في الاحوال

— 100 —



Switch>en

Switch # Config T

Switch(Config) # Banner motd # Hello #

من الملاحظ اننا نكتب اشارة بسم علامتيه غير يغير مثل مثل علامه الدولار مثلا #

## Switchport modes

ينقسم المود الخاص بالبورت في السويتش الى Access و Trunk

- البورت الذي يتصل به جهاز كمبيوتر ليس Access

- البورت الذي يتصل به جهاز سويتش آخر ليس Trunk

- عند توصيل جهاز الكمبيوتر بالسويتش يتعرف السويتش على البورت تلقائياً أنه Access

لكن في بعض الاحيان لابد من اعداد الامر على السويتش لكي يتعرف على البورت أنه Access

وتنقسم الامر في حاله Trunk

\* لجعل السويتش يقرأ البورت على أنه Access أو Trunk

Switch>en

Switch # Config T

Switch(Config) # int Fa/1

Switch(Config-if) # Switchport ~~Access~~ mode Access

Switch(Config-if) # Switchport mode Trunk

طريقه حل خطبه الكمر او لا نستخدم الامر show run في كل خطبه ام لا

Switch # show Run



## Port Security

تعتبر خاصية حماية مخرجات الشبكة من التغير في التكوين من البورت من التشخيص الاستثنائية التي  
تتمثل في البورتات ولفظهم ذلك تضمنت أنه ستحذف ما على الشبكة أو زوال الجهاز المتصل على  
الترقية من العمل وإذا جاز آخره ذلك الذي يجب الحذف من وقتاً يتوصل به بالكلية الخاص  
بالجهاز الأصلي الذي أزاله من الشبكة من هذه الحالة قد يقوم هذا المخدم بجعل أو سن  
بعض الشبكة أو ربما يزيل الشبكة نفسها من هذه الحالة من تأنيلاً فكل تقاض هذه المشكلة  
من استخدام port security وهذا باضطرار لو تم تغيير المالك الخاص بجهاز الكمبيوتر المتصل  
بالسويتش يقوم السويتش بإزالة البورت من لوقتاً الشفط بإعادة الجهاز الأصلي  
الذي به الـ mac address المحفوظ عليه من قبل السويتش فإنه السويتش له يضع البورت مرة ثانية  
إلا أنه فلول الدعم - به تلك هي فكرة الـ port security

تفعيل خاصية الـ port security

[1] تحديد البورت على أساس الـ Access

```
Switch(Config) # int Fa/1
```

```
Switch(Config-if) # Switchport mode Access
```

• بفرقنا أنجز أكثر من بورت من مخرج متتالية من رقم أمر Range

```
Switch(Config) # int range Fa/1 - 5
```

```
Switch(Config-if-range) # Switchport mode Access
```

• بفرقنا أنجز أكثر من مخرج كلة غير متتالية

```
Switch(Config) # int range Fa/1, Fa/3, Fa/5
```

```
Switch(Config-if-range) # Switchport mode Access
```

[2] إعداد خاصية الـ port security

```
Switch(Config-if) # Switchport port-security
```

[3] تحديد الماك المراد تثبيته وحفظه

```
Switch(Config-if) # Switchport port-security mac address
```



تكتب بهذا الخطوط رقم (١٢) أني قد وكيتي هذا على شجرة المالك حي  
أنه بغير هذا الأمر من ١٢ إلى ٢٠ جهات قد يكون ذلك إلى أن يكون عنوان  
رقم ١٢٤٤ معيد ولذلك فتطيع تكتب هذا الخطأ على طريقه أمر جيل السوريش



# # Mac address Maximum

قد نلاحظ عند مراقبة الـ MAC address في الـ switch على نفس الـ port

(مثال)

أجهزة (VLAN) وهذا يارر أنه أجهزة تطبقه ناهضوا أنه لا تستخدم وقت يتم توصيلها بالـ switch والفرق يتم توصيلها بالـ switch كما بالـ switch



فإن هذه الحالة الـ switch متصل عليه أكثر من 2 MAC ولهم المالك الخاص بالـ switch وإزالة الخاص بجهاز الكمبيوتر عند قطع أنه جعل الـ switch يقرأ كل المالكه أو أكثر من 2 MAC استخدام خاصية # Mac address maximum

Switch (config-if) # switch port port-security maximum 2

Switch (config-if) switch port port-security mac address

ولإضافة المالك الثاني وفي الأمر وتكتب المالك الثاني وخاصية الزيادة في switch على الـ switch

## خاصية Violation

كلمة Violation عن انتهاك أو اختراجه والمراد هنا الإجراءات التي تتخذ عند حدوثه معية اختراجه للـ switch أو استقبال الجهاز المعرف على الـ switch من هذه الحالة يكون هناك ثلاث إجراءات

Shut down	protect	Restrict
↓	↓	↓
يتم إغلاق الـ switch عند استقبال الجهاز حين ولو تم إعادة الجهاز الأصلي فإنه الـ switch سيقطع مفعله	يتم إغلاق الـ switch عند استقبال الجهاز كونه معية يتم إعادة الجهاز الأصلي فإنه الـ switch سيقطع مفعله	تتم فكرة عمل الـ protect كمنع إرسال رسالة للأجهزة عند اختراجه
عندما يقوم الـ switch بفتح مفعله أو غير	عندما يقوم الـ switch بفتح مفعله أو غير	عندما يقوم الـ switch بفتح مفعله أو غير
De fault	De fault	De fault

لتغيير الـ protect أو Restrict

switch (config-if) # switch port port-security violation protect Restrict mode



## Port Security - ١١

Switch > en

الواجهة F0/1

Switch # Config t

Switch (Config) # int F0/1

(تحت الواجهة)

Switch (Config-if) # Switchport mode access

(تحت الواجهة)

Switch (Config-if) # Switchport port-security ~~mac address~~

(تحت الواجهة)   
 (تحت الواجهة)   
 (تحت الواجهة)

Switch (Config-if) # Switchport port-security mac address

(تحت الواجهة)   
 (تحت الواجهة)   
 (تحت الواجهة)

أو sticky   
 (تحت الواجهة)

Switch (Config-if) # Switchport port-security mac address sticky

(تحت الواجهة)

Switch (Config-if) # Switchport port-security maximum 3

(تحت الواجهة)   
 (تحت الواجهة)

Switch (Config-if) # Switchport port-security mac address ex1

Switch (Config-if) # Switchport port-security violation shutdown

Switch (Config-if) # exit

(تحت الواجهة)   
 (تحت الواجهة)

Switch (Config) # exit

Switch # show port-security address

(تحت الواجهة)   
 (تحت الواجهة)

[C] للتعامل مع أكثر من ١٠

Switch > en

Switch # Config t

Switch (Config) # int range F0/1-5

(تحت الواجهة)

Switch (Config) # int range F0/1, F0/3, F0/5

(تحت الواجهة)

Switch (Config-if-range) # Switchport mode Access

(تحت الواجهة)

Switch (Config-if-range) # Switchport port-security

(تحت الواجهة)

Switch (Config-if-range) # Switchport port-security mac address sticky

Switch (Config-if-range) # Switchport port-security maximum 3

(تحت الواجهة)

Switch (Config-if-range) # Switchport port-security violation shutdown

Switch (Config-if-range) # exit

Switch (Config) # exit

Switch # show port-security address



Switch (config) # shutdown

Switch (config) #

Switch (config) #

Switch (config) # int F0/1

Switch (config -if) # shutdown

Switch (config -if) # No Shutdown

توقف البورت

توقف shutdown وجعلها

No shutdown جعل

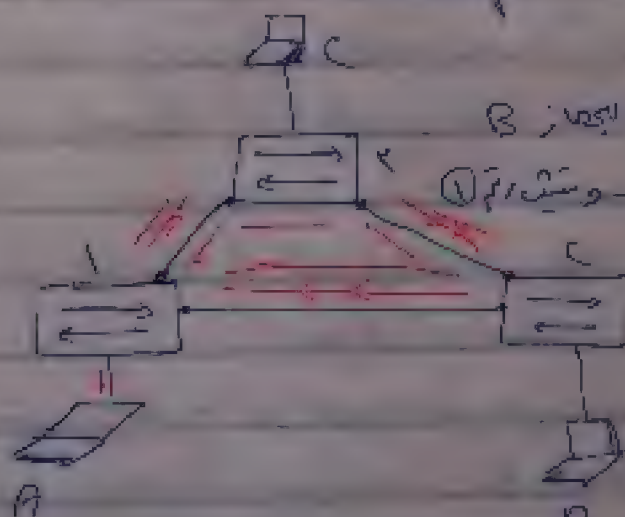
## Spanning Tree Protocol

### STP

هذا هو اسم بروتوكول الـ Switching وله أيضاً اسم آخر وهو اسم  
عالم له وهو 802.1d

وبروتوكول STP هو بروتوكول خاص به يعمل على تجنب حدوث حلقات Loop avoidance وهو يعمل بصورة أوتوماتيكية وهو يعمل على تقليل حدوث الحلقات Loop avoidance

مثال لفهم عمل الـ Loop



بفرض أنه الجهاز A يرسل رسالة للجهاز B

فإن الرسالة تخرج من A إلى B وتستقر في B

الذي يقوم بإرسالها للسويتش

الذي بدوره يرسلها إلى B

وهو يرسلها إلى B

وهو يرسلها إلى B

تفقد الجهاز A رسالة تتبعها جزئياً الرسالة الكابلات مما يؤدي إلى فشل الشبكة وهو ما يعرف  
بـ Loop

في المثال موضح أنه يوجد حلقة في الشبكة ولكن بوجود التوجيه لا يحدث Loop

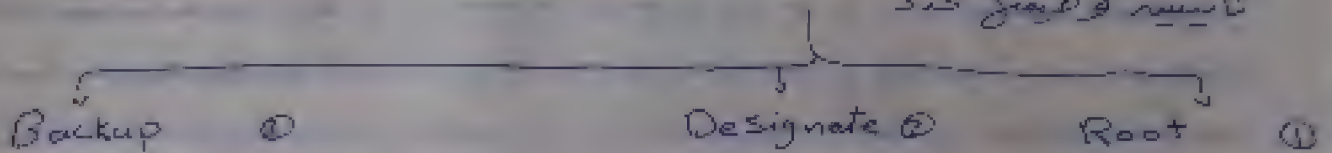
فيكون STP يتفعل بطريقة واحدة ويمنع التكرار بين الأجهزة تلقائياً أو تلقائياً



من المشكلة هنا ان Loop

خاصية ال Bpdu

نظر افتراض Bridge protocol data unit و هو عبارة عن رسالة يتم ارسالها كل ثانيته وتحتوي عدد



ولفهم هذه المصطلحات نوضح مثال

نفرض اننا نضم ههنا صانعة ادوار يوجد سويتش مركزي من العاتا سيقتر يكونه سويتش مركزي ليس Root ادوار الاخرى لا تستطيع ان امد كابلات للأجهزة من كل جهاز ال Root صا حرة لكن لا نزم ان يكونه من كل دور منه المين سويتش خادم لهذا الدور ويتم توصيل هذا السويتش "designate" بالجهاز المركزي وهو ال Root وهذا من كل ادوار المين.

وظيفة Bpdu هي ان رسالة كل ثانيته يتم بارسلها كل سويتش لكي يحصل على ال mac address الخاص بكل سويتش عن طريق هذه الرسالة فيستطيع السويتش ان يحدد دوره هل هو Root او designate

ولمعرفة كل السويتش Root او designate نستخدم الأمر show

Switch # show spanning-tree

سيفر لنا كل السويتش Root او designate حيث انه يظهر المالك الخاص

بالسويتش الذي نفذت عليه الأمر عنوان ex Bridge ID Address

ويظهر الجهاز ال Root عنوانه ← Root ID

ويكون المالك الخاص به هو ex لكن يعرف اننا نفذت

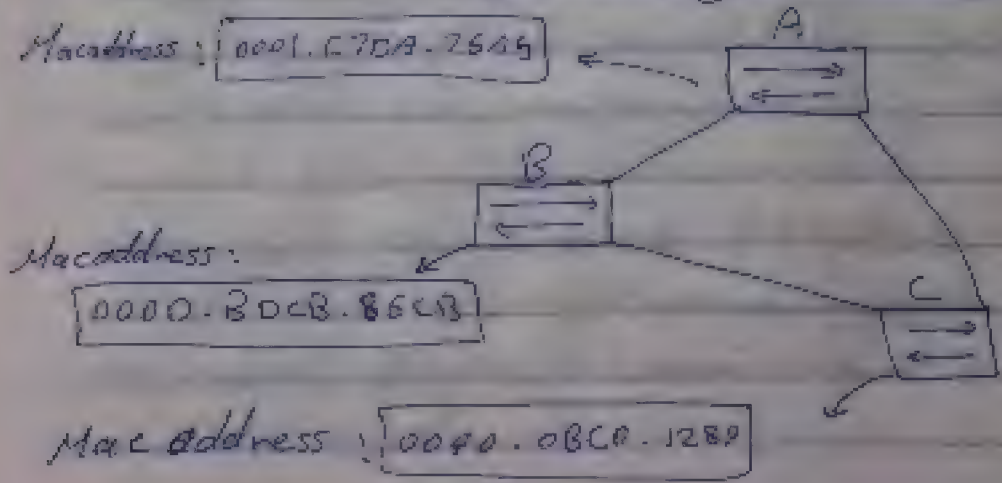
الأمر على جهاز ال Root - يظهر في رسالة توتر أن الجهاز هو ال Root

ونلاحظ انه Bridge ID Address & Root ID Address بنفس العنوانه ex

كيفية تحديد الجهاز الـ Root • Designate

يتم اختيار الجهاز الـ Root على أساس أرقام الـ MAC address

ولفكر عملية أكثر ملاءمة Mac address نوضح المثال التالي



نلاحظ من المثال أنه السويتش [A] عنوانه الملك الخاص به يبدأ بـ 0001 مجموعهم

1 + صفر + صفر + صفر = 1 ونلاحظ أنه الجهاز [B] عنوان الملك يبدأ بـ 0000

منفردون بتحويل الـ D إلى 13 حيث أنه رقم الملك هو رقم سداسي عشري hexadecimal  
 A B C D E F 10 11 12 13 14 15  
 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

الخاص بالسويتش B = 12 + صفر + صفر + صفر = 12 فيكونه A أقل منه B وبالنسبة

للجهاز [C] عنوانه الملك الخاص به هو 0040 فيكونه صفر + 2 + صفر + صفر = 2

فيكونه أيضاً A أقل منه B و C

لذلك يكون الجهاز A هو الجهاز الـ Root والأجهزة

B و C هي الأجهزة الـ Designate

**هنا** هذه الرسالة Bpdu تقوم بفتح أبواباً يمكن تقديمه منه هو الجهاز الـ Root ومنه الـ Designate وعندما ينتهي تقديمه منه هو الرتبة Root لا تقوم السويتشات الأخرى بإرسال رسالة Bpdu ويقوم جهاز الـ Root فقط بإرسال هذه الرسالة. كل تانيته للتحقق باقرا الأجهزة أنه هو الرتبة حيث تكون الرسالة على الملك الخاصة به



## مقدمة عن redundancy

الهدف من redundancy هو توفير أمان وبقاء الشبكة  
 اختيار واحد من بين عدة مسارات لتصل من المصدر إلى الوجهة  
 مع العلم ان كل مسار له تكلفة مختلفة وتختلف هذه التكلفة باختلاف  
 سرعة النقل ووقت التأخير في كل مسار.  $\text{Cost}$  هو القيمة التي  
 تمثل هذه التكلفة وتختلف باختلاف المسار. الهدف من redundancy هو  
 توفير بديل في حالة فشل المسار الرئيسي.

وتجدر الإشارة الى ان redundancy لا يتم بروتوكول  
 STP بالاعتماد على واحد المسارات بصورة مؤقتة وفراغالة  
 بل يتم بروتوكول STP التناوب بين مسارات التناوب فلا تتأثر  
 الشبكة بتلفها المسار الأول.

لنقدم هذه العملية لاسباب فوضع أمور

1. Root هو الجهاز صاحب أقل Mac address وهو الذي سكرهنا سابقاً
2. Designate هو الجهاز الذي بدوره سيراد Root وتسمى هذه Non-Root Bridge
3. في البورتات على جهاز الروت تسمى Forward port وأما Designated port
4. Root port هو البورت يكون في الجهاز Designate ويكون صاحب أقل قيمة  
 على كل تكلفة البورت الروت أو ان تكون مرتبطة مع Root

• إذا كان لدينا أكثر من  $\text{multicasting}$  يقوم الـ STP باختيار Root port  
 واحد من البورتات وطريقة الاختيار تكون اختيار أقل  $\text{Cost}$  (القيمة)  
 بالنسبة للـ Cost وهو التكلفة

بالنسبة لرقم البورت

F0/1

F0/2

F0/3

Speed | Cost

10G

2

G-E

4

F-E

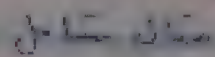
19

E

100

إذا كان لدينا أكثر من التكلفة للوصول بروتات السويتش الى Designate

6. 10. 1951

[illegible]

1- Root هو الجذر،  $A \Rightarrow$  صاحب أقل mac كما يتفاد التكاليف  
 2- Rootport ~~هو~~ <sup>Designated Forward</sup> هي البورتات  $Fo/1$  و  $Fo/2$  لدى بورتات الجذر، الـ Root  
 3- Rootport الخاص بالجذر C هو البورت  $Fo/3$  لأنه صاحب أقل تكلفة من الوصول  
 إلى الجذر الـ Root

2- في Rootport الخلف بالجهاز B هو البروت F0/6 لأنه صاحب أقل تكلفة من الوصول للجهاز الـ Root

٥. Designated port (DP) : الناص بالوصلته بين السويتش B و C هو صاحب أقل مارجين  
 و أصبح لنا ٣ أمثل مارجين هو C متبوعه F0/15 هو (DP) أو ال Designated port  
 ٦. Block port (BP) : وهو البورت الأخير الذي ليس Root port (RP) أو ال Root port  
 ٧. Designated port (DP) : ويكون هو البورت F0/15

\* هذا المثال يوضح فكرة عمل الـ  $STP$  والإخانة قبل بشكل تلقائي.



# إعداد سوويتش معين لي انا يكونه هو ال Root

لجعل جهاز معينه كى يكون هو ال Root بقا ز الروت قلينه اعدى صفحت الاضافات ونادى  
ال Ethernet به انا من قبله منك انا Ethernet تتبع الامور التاليه

```
Switch > en
Switch # Config T
Switch (Config) # Spanning-tree Vlan 1 Root primary
```

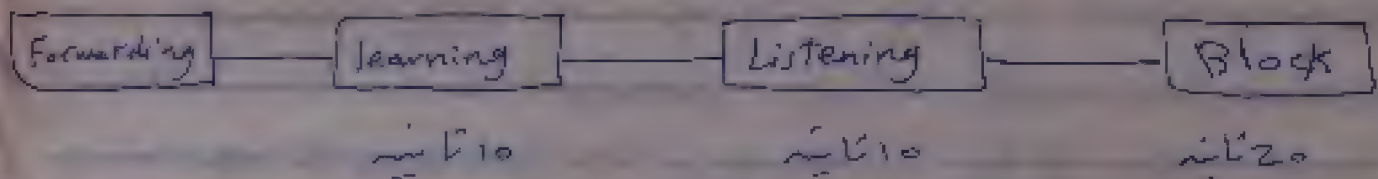
بالتالى هذا الامر يصح هذا السويتش هو الروت حلفه هل اصبح الروت ولدك

```
Switch > en
Switch # show spanning-tree
```

نتعرف اننا اصبح هو الجهاز ال Root

# خاصية ال Rapid pvt

وقتها من على ال Redundancy انه الكابل القالب بين سويتش ال STP باستقبال  
العمل على الكابل البديل كله عليه الاستقبال يتم فى بعض التأخير حيث اننا فى  
بعد مراحل تأخذ حواس 20 ثانية مقسمة الى



بعد مرور حواس 20 ثانية يعمل الكابل البديل مكانه الكابل القالب كله هذه المدة من ال  
التيكات والى العمل فتعود الى مكانه كل سويتش هذه المشاكل نستقيم خاصية  
Rapid-pvt التي تجعل الكابل يعمل مكانه الكابل القالب مباشرة دونه انتظار 20 ثانية  
كله فعل هذه الخاصية تتبع الامر الاخرى ال أجهزة السويتش سواء ال  
الجهاز ال Root أو الأجهزة الأخرى ال Designate

## مقدمة في Rapid-PST

Switch > en

Switch # Config ?

Switch(Config) # Spanning-Tree mode Rapid-pst

وتفعل الأمر على كل السويتشات لأنه إذا قام هناك أحد السويتشات بالرفع

العودة إلى pst فإنه لن ينجح سيعمل على هذا الوضع ولن يتغير الوضع السريع له

أما تفعل rapid-pst على كل السويتشات

## VLAN

أما VLAN هي اختصار Virtual LAN أي شبكات داخلية وهمية  
تفكر على ذلك VLAN توضح هذا المثال التالي :



تفكر أن VLAN هي إمكانية اعتبار الجهازين A و B شبكة منفصلة عن الجهازين C و D  
فإذا أرسل A و B سيصلها B فقط وإذا أرسل C و D سيصلها D فقط رغم  
أنهم جميعاً مشتركين في سويتش واحد

## نوائد الـ VLAN

1- تقليل عملية الـ Loop

2- تقليل الازدحام بين عناوين Subnet أكثر من Subnet أي أن تقسم الأجهزة لشبكات منفصلة

3- حل مشكلة physical limitation أي لو كان السويتش طياراً فإصدار شبكة شتري

تابع لتقسيم القسم في سويتش آخر وأرابطهم معهم

4- تستطيع جميع أجهزة قسم معين في الشبكة واحدة حتى لو كانوا في أماكن مختلفة أو سويتشات مختلفة



[illegible]

مبدأ البروتوكولات الخاصة بالـ VLAN



24

هو برو تولد وانه گمانه خاصا بغير كفة مستعملو  
ان ابي و انك و تنصع باستقامه صيغه  
عيونه اكثر من هنرايه

فصل فی بیان احوال و مشیقات

على مقتضىات الـ *Trusts* حيث يقوم البروتوكول  
بتفصيل بيانات الـ *Trusts* على السوريش الاول  
وتفصيل على مقتضىات الـ *Trusts* حيث يدل  
الى السوريشات الاخرى ويكرر على ذلك.



هذه البرقيات نقل بحرية ارتوجاسكية

معظمته الى الامم المتحدة على السويش نأتمم الامم المتحدة

switch > on

```
Switch# show vlan
```

قبل إنشاء VLAN - مقر لها Default VLAN وهي VLAN 1

تجعل جميع النخبة المتصلة على السويقتين ترى بعض البعث لذلك مستقر لنا وصيقل  
أمر جميع البعثات على السويقتين صريحة تحت هذه الأمثلة

$$\sqrt{L_A N_1}$$

## VLAN Configuration

ترجمة: إنشاء VLAN جديد

192.10.10.0

① تحديد عنوان الشبكة لكل VLAN

② تحديد IP الأجهزة تحت عنوان VLAN مثل 192.10.10.1 PC → SP →

③ إعداد السويتش

④ تسمية الـ VLAN

⑤ إعداد VLAN

⑥ تسمية البورتات الـ Trunk

⑦ تسمية البورتات الـ Access

⑧ إدراج المفاتيح الخاصة بالأجهزة تحت الـ VLAN فاصلة

① إنشاء الـ VLAN

Switch > en

Switch # Config T

Switch (config) # VLAN 2

② تسمية الـ VLAN

Switch > en

Switch # Config T

Switch (config) # VLAN 2

Switch (config-VLAN) # Name Accounting



## ② كيفية البورتات Access

Switch > en

Switch # Config - T

Switch (config) # int Fa/1

Switch (config - if) # Switchport mode Access

في حالة أنترميديوت متكامل

Switch (config) # int range Fa/1 - 4

نقطة

Switch (config - if - range) # Switchport mode Access

في حالة أنترميديوت غير متكامل

Switch (config) # int range Fa/1, Fa/3, Fa/5

نقطة

Switch (config - if - range) # Switchport mode Access

## ③ كيفية البورتات Trunk

Switch > en

Switch # Config T

Switch (config) # int Fa/1

نقطة

Switch (config - if) # Switchport mode Trunk

في حالة أنترميديوت متكامل أو غير متكامل نستخدم Range كما في البورتات Access

## ④ ادراج البورتات الخاصة بالأجهزة مع كل VLAN الخاصة بتجهيز

Switch > en

Switch # Config T

Switch (config) # VLAN 2

Switch (config - vlan) # Name Accounting

Switch (config - vlan) # exit

Switch (config) # int Fa/1

نقطة

التي  
تسمى  
تسمى

## تكوين الـ VLAN

Switch(Config) # int Fa/1

Switch(Config-if) # Switchport Access VLAN2

صنعنا البورتات من 1 إلى 4 تتبع الـ VLAN2  
فإنها الآن البورتات من 1 إلى 4

Switch(Config) # int range Fa/1 - 4

Switch(Config-if-range) # Switchport Access VLAN2

صنعنا البورتات من 1 إلى 4 تتبع الـ VLAN2  
فإنها الآن البورتات من 1 إلى 4

Switch(Config) # int range Fa/1, Fa/3, Fa/5

Switch(Config-if-range) # Switchport Access VLAN2

صنعنا البورتات من 1 إلى 5 تتبع الـ VLAN2

## # بعض الاوامر الاخرى

- لعرض الـ VLAN الموجودة في السويتش وان البورتات تتبع الـ VLAN

Switch > show

Switch # show VLAN

- لعرض البورتات التي تقع على الـ Trunk

Switch # show interfaces Trunk

- لعرض خصائص الـ بورتات في الـ Show run

Switch # show run

سيفرض الـ بورتات تتبع الـ VLAN

- لاضافة وصف الـ description لـ الـ بورت

Switch(Config) # int Fa/1

الـ بورت

Switch(Config-if) # description connected to VLAN2

مثال

Switch(Config-if) # exit

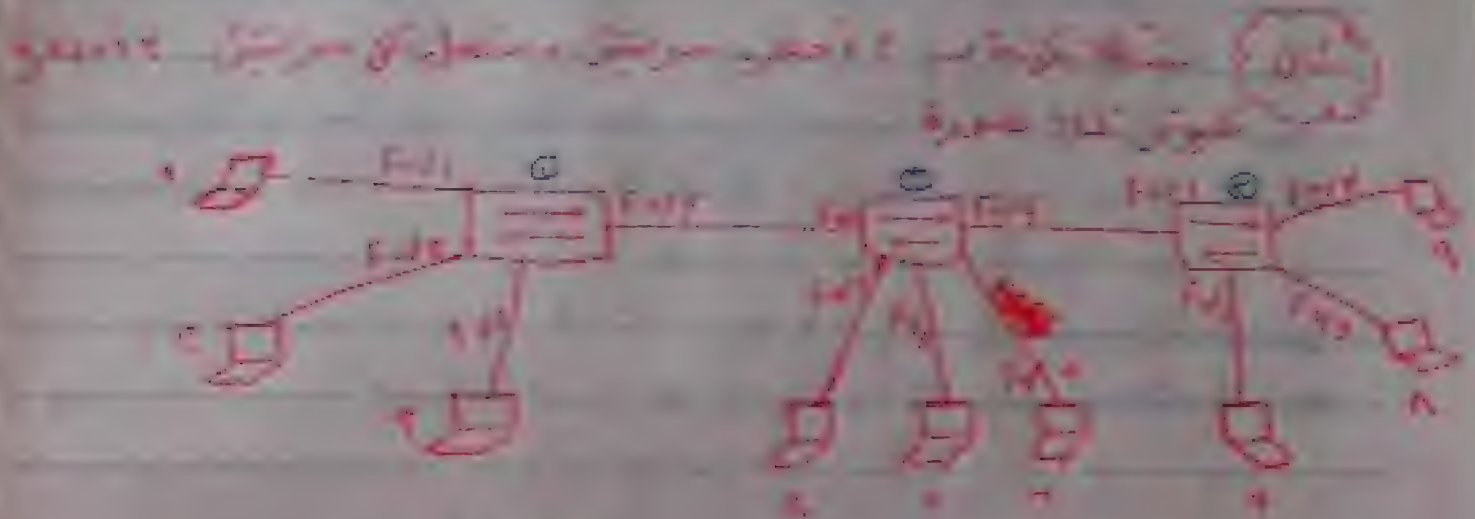


لو افعلنا الأمر بـ VLANs

Switches of Sales & IT

نظمنا أجهزةنا وبنينا تحت VLANs في أجهزةنا وبنينا تحت VLANs

وVLANs تحت VLANs في كل من الشبكات المختلفة



بـ VLANs الأجهزة التي هي حاسوب و 3 أجهزة حاسوب أخرى  
و 3 أجهزة حاسوب أخرى و 3 أجهزة حاسوب أخرى  
و 3 أجهزة حاسوب أخرى و 3 أجهزة حاسوب أخرى

الاجابة

أولاً نضع في الشبكات أتنا سوف نقوم بإنشاء 3 شبكات VLANs وهي

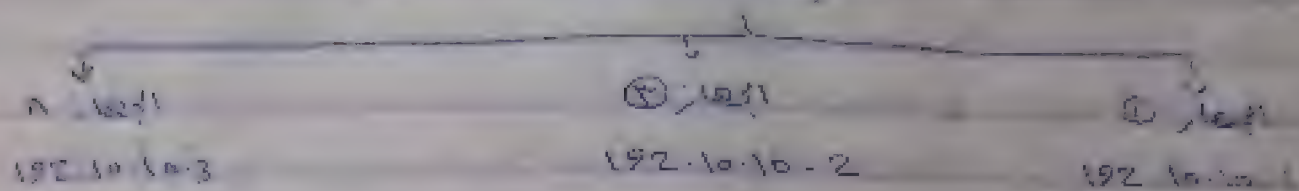
Accounting ① Sales ② IT ③

① تحديد عنوان لكل VLAN

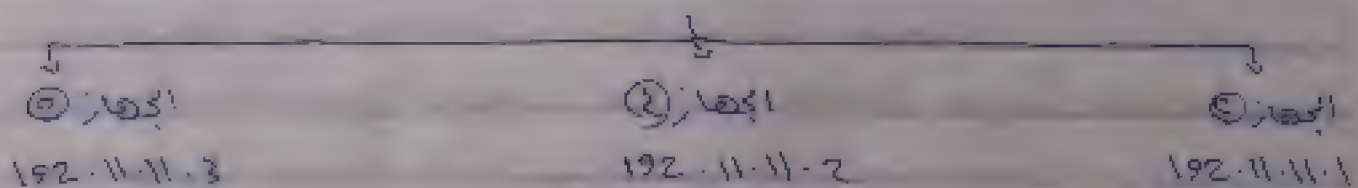
- Accounting 192.10.10.0
- Sales 192.11.11.0
- IT 192.12.12.0

المسألة ١١ - ٢٨ - VLAN في جهاز سويتش (٢)

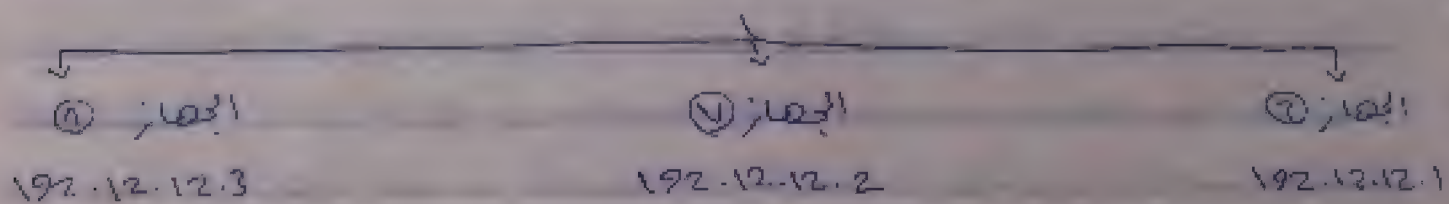
### Accounting



### Sales



### IT



٣) أوامر ال Configuration الخاصة بكل سويتش

١) الجهاز ١

Switch > en

Switch # Config T

Switch (config) #

• إنشاء وتسمية ال VLANs

Switch (config) # vlan 2

Switch (config-vlan) # Name accounting

(Accounting)

Switch (config-vlan) # exit



Switch(Config) # int Fa 0/24

Switch(Config-if) # name Sales (Sales)

Switch(Config-if) # exit

Switch(Config) # vlan 2

Switch(Config-vlan) # name IT (IT)

Switch(Config-vlan) # exit

\* تحديد البورتات الـ Access و البورتات الـ Trunk  
هذه المرحلة الأجهزة (PC) تكون متصلة بـ Access و البورتات الـ Trunk  
تكون Trunk

Switch(Config) # int range Fa 1/1-3

Switch(Config-if-range) # switchport mode Access

هنا البورتات 1-3 هي البورتات Access

Switch(Config) # int Fa 1/4

Switch(Config-if) # switchport mode Trunk

هنا البورت Fa 1/4 هي البورت Trunk

\* ادراج كل بورت تحت الـ VLAN الخاصة به

Switch(Config) # int range Fa 1/1, Fa 1/3

Switch(Config-if-range) # switchport Access VLAN 2

هنا البورت Fa 1/1 و Fa 1/3 هي البورتات مع VLAN 2 و هي الـ Accounting

Switch(Config) # int Fa 1/2

Switch(Config-if) # switchport Access VLAN 3

هنا البورت Fa 1/2 هي البورت مع VLAN 3 و هي الـ Sales

انتصيا من الـ configuration الخاصة بالسويتش رقم واحد (1)  
والنسخة للسويتش رقم 2 لا يمكن نسخها

لا يمكن ان يكون الـ VLAN خاصا

① تحت البورتات الـ Access والبورتات الـ Trunk

② ندرج كل جبهة تحت الـ VLAN الخاصة به

وطهره ما تم انشا له على السويتش. فنقدم الأمر

`Switch# show vlans`

سيوضح هذا الأمر الـ VLANs الماشي والبورتات الخاصة بكل VLAN

**ملاحظة** من هذا المثال لا بد لنا أنه نقوم بعملية الـ Configuration على كل جهاز  
من أجهزة السويتش لكن هذه العملية قد تكون متعبة ومضنية  
نظرا لاختلاف أماكلا السويتشات وقد يؤدي كثرة الـ Configuration إلى خطأ  
أو اللطأ في بعض  
لذلك نحتاج نظاما تلافى تلك المشكلة عبر طريقة استخدام بروتوكول VTP

VTP

بروتوكول الـ VTP هو اختصار عن الـ VLAN Trunking protocol  
وهو بروتوكول خاصا يستخدم لنقل عمل الـ configuration هو أنه عند انشاء الـ Configuration  
على سويتش معين يقوم هذا البروتوكول عند تفعيله بإنشاء ونسخة من الـ Configuration  
على باقي السويتشات مما يوفر الجهد والوقت.

وبالرغم من أنه يوفر هذه المزايا إلا أنه سيكون قاصدا بعضا من عيوبه نظرا لأنه  
لوحدث خطأ في الـ configuration في السويتش سيؤثر هذا البروتوكول على باقي  
الـ configuration ما قبل الخطأ ونسخه على باقي أجهزة السويتش

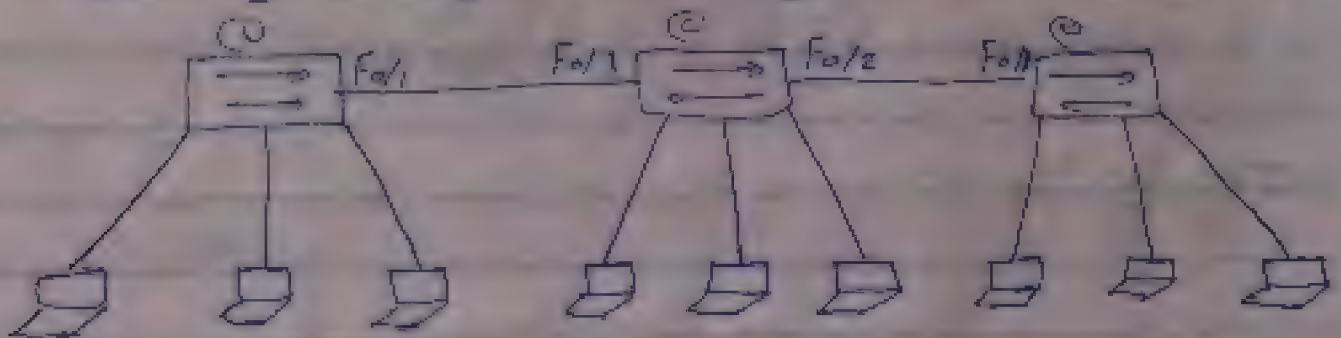


## \* تفعيل VTP

- ① تعريف البورتات التي تربط السويتشات مع بعضها على أن تكون Trunk
- ② إنشاء Domain وتكونه بنفس الاسم على كل السويتشات وإعداد كلمة سر على كل السويتشات
- ③ تحديد جهاز واحد على أنه الجهاز الـ Server وهو الذي يكون عليه كل الـ VLAN عليه

### شرح العناصر السابقة بالتفصيل

- ① تعريف البورتات على أن تكون Trunk وتقع بين الترتيب بين السويتشات



Switch 1 en

Switch # Config T

Switch (Config) # int Fa/1

Switch (config-if) # switchport mode Trunk

هذه هي البورت Fa/1 الذي يربط السويتش ① بالسويتش ② لكي أنه Trunk وتعمل نفس الخطوة على كل البورتات التي تربط بين أجهزة السويتش ويعمل العنصر الأخير على أنها بورتات Trunk

## ② إنشاء Domain باستخدام VTP

قبل أن نبدأ نلاحظ أننا نحتاج أن يكون لدينا Switch واحد على الأقل  
 Switch # show vtp status

ونظهر لنا بعض المعلومات الخاصة ببروتوكول VTP من خلال:

VTP operating mode	: Server
VTP Domain Name	: <u>أحمد</u>

نلاحظ هذه النقطة من العنود التالية

نلاحظ أن DomainName فارغ وأن نقوم بتفعيل بروتوكول VTP لدينا  
 نحن DomainName ونعني به كلمة DomainName لا يتبع أي اسم من Configuration  
 إلى أن نكتبه جديد إلا بعد إدخال كلمة السر

## ③ إنشاء DomainName وكلمة السر

```
Switch >en
Switch # config T
Switch (config) # vtp mode Server
Switch (config) # vtp domain Ahmed
Switch (config) # vtp password 1234
```

عند إنشاء Domain ونلاحظ أنه يكون من البداية DomainName فارغ كلمة السر  
 تسمى باسمه اسم تقوم السويتشات الأخرى بالاتصال لذلك إلى Domain بها صورة

Switch # show vtp status

على السويتش الثاني أو الثالث من المثال السابق نجد الصورة كالتالي

```
VTP operating mode : Server
VTP Domain Name : Ahmed
```

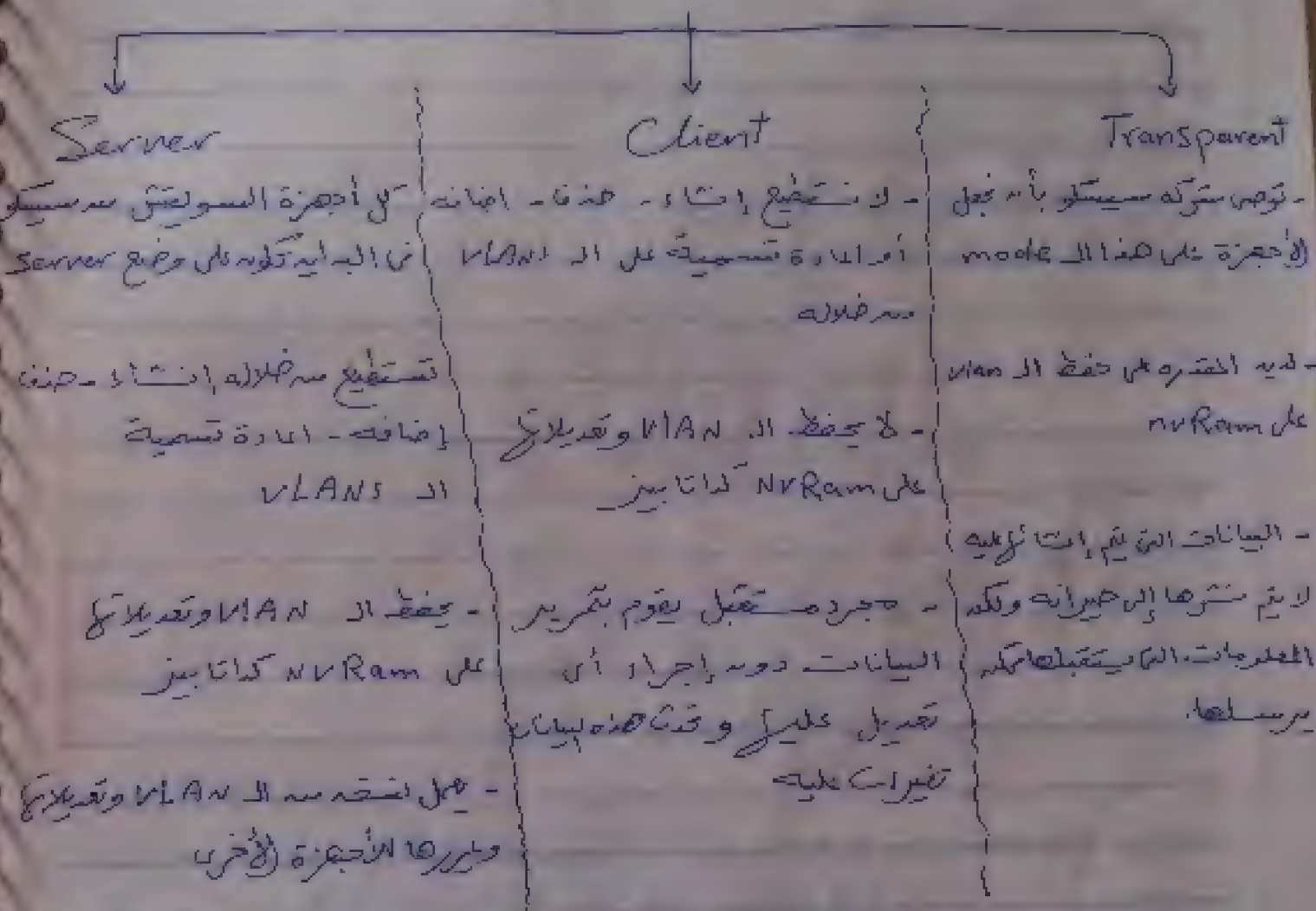
أي أنه يجب الـ DomainName وأنهم ليس مجرد إنشاء لأنه في الأصل فارغ  
 فلا وجه إنشاء Domain قتل السويتش الاتصال إليه بدل من أن يكون فارغ



⑤ تقسيم الجهاز الذي لم يانشأ الـ VLAN عليه على أنه الـ Server والباقي من أجهزة السويتش Client

هناك ثلاثة أنواع لهذه التقنية الـ Server الـ Client وTransparent

### VT modes of operation



بعد أن ختمنا الفرق بين Server و Client و Transparent

لابد أن نذكر أن جهاز واحد الـ Server هو الجهاز الذي نقوم بإنشاء الـ VLANs عليه والباقي Client

خطوات عمل Server

Switch>en

Switch># config t

Switch(Config)# vtp mode server

ملاحظة: يجب تغيير الموقع إلى Default وتبديل اسم VLAN على الجهاز  
الذي نشأت عليه الـ VLAN

\* خطوات عمل الجهاز Client وتغيير الـ Domain و الـ password

Switch>en

Switch># config t

Switch(Config)# vtp mode client

Switch(Config)# vtp domain Ahmed

Switch(Config)# vtp password 1234

بعد الخطوات التالية

1- إنشاء الـ configuration الخاصة بـ Mode Trunk للجهاز الـ السويتشات

2- إنشاء الـ Domain name والـ password

3- تعريف الـ switch 2 على أنه Client

4- لعملنا أمر Show vlan سنقوم الـ VLAN على السويتش 1

على الجهاز رقم 2 لأننا فعلنا الـ VTP

الخلاصة

يتم عمل الـ VTP في الـ VTP هو إنشاء الـ VLAN على السويتشات

الأخرى بعد اتباع الخطوات السابقة.

\* VTP هو بروتوكول غير آمن حيث يمكن أي شخص أن يحصل على إعدادات

الـ VLAN بمجرد اتصاله بالسويتش عبر طريقة جورت Trunk

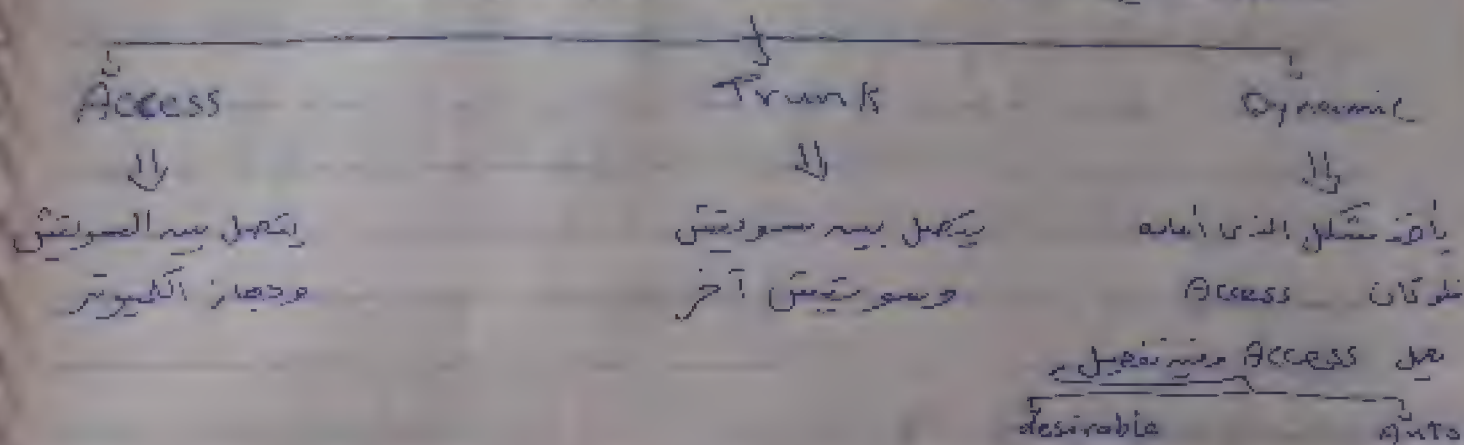
وهذه الطريقة تلتزم الأمان التي تجعله سويتش Client ولكن نتعلم



**DTP**

## Dynamic Trunking Protocol

تفادى هذه المعضلة قد أنه نرى ما نسميه *expected trunking operational mode*  
 ولقد تم الصياغة السابقة لانه نعلم أنه البورت يكون إما



الآن سترسم جدول يوضح فيه الحالات

يقابل	Access	Dynamic Auto	Trunk	Dynamic Desirable
Access	Access	Access	<u>Dont use</u>	Access
Dynamic Auto	Access	Access	Trunk	Trunk
Trunk	<u>Dont use</u>	Trunk	Trunk	Trunk
Dynamic Desirable	Access	Trunk	Trunk	Trunk

شرح آخر للجدول

- ① بورت Access أمامه بورت Access النتيجة Access
- ② بورت Trunk أمامه بورت Trunk النتيجة Trunk
- ③ بورت Trunk أمامه بورت Auto النتيجة بورت Trunk
- ④ بورت Trunk أمامه بورت Desirable النتيجة بورت Trunk
- ⑤ بورت Access أمامه بورت Dynamic النتيجة Access

تظهر خطورة هذا الجدول في حالة أنه يفرض أنه البورت في المودم الذي  
 يعمل بجهاز كمبيوتر من السابقة كانه D-Desirable فلو قام

[illegible]

قائمة للأدوات المستخدمة في البرمجة في المونتاج في الشبكة Dynamic Analysis  
تغيير البرنامج (PC) وجعل مكانه حقيقي وجعل البرمجة في المونتاج في الشبكة Dynamic Analysis  
Dynamic Analysis في البرمجة في المونتاج في الشبكة Dynamic Analysis في البرمجة في المونتاج في الشبكة Dynamic Analysis  
في سطح الوصول إلى هذه البيانات

خلال هذه الفترة

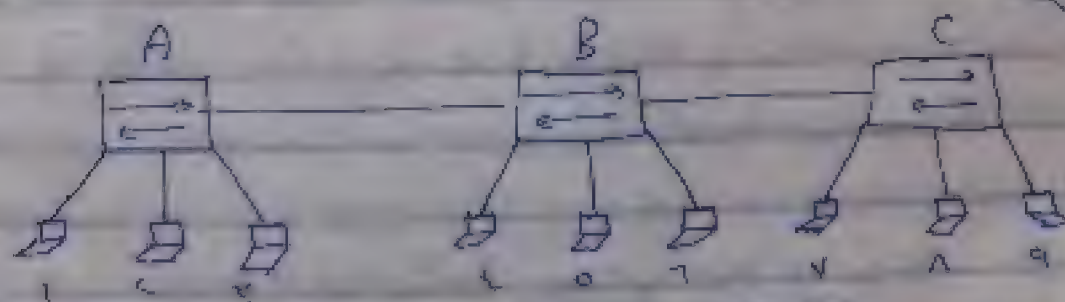
يتم علاج هذه المشكلة من تعريف البورتات التي تصل إلى أجهزة الشبكة (PC) على أن البورتات Access بالتالي لا يستطيع أحد أن يحصل على بيانات الـ VLAN إلا أنه طرعي سويفتات المشكلة والتي طبعا يكون لها -- مورد خيالي معلن الحماية على الـ VLAN وضع أيضا معالج المقادير البورتات مع طرعي الأمر switchport nonegotiate (config - if) switch

# خصائص پروتوکول VTP

Frame Tagging (1)

يقوم بروتوكول الـ VTP بوضع Tag أو علامة على الـ Frame  
كل من بينهم السويتش الـ Frame متجهة لشب. أجهزة

12



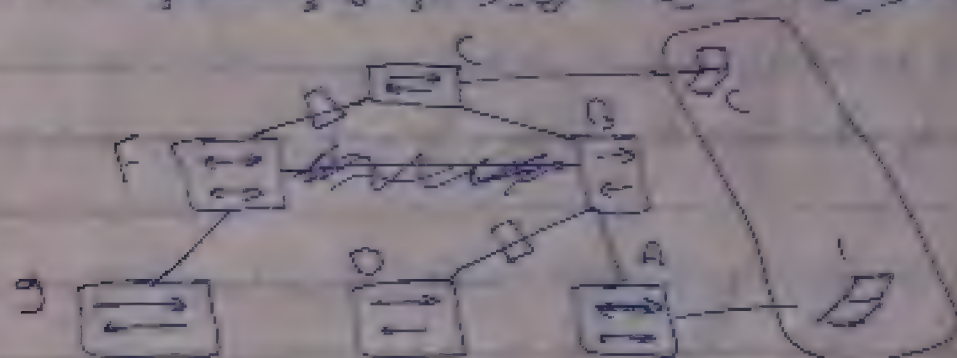
بصرفه أنه الأجرة  $n \leq c$  تبع  $v/m \leq c$  اوقات الجهاز رقم ① بالرسالة



الـ Frame إلى الجهاز A وإدخال Frame يخرج من السويتش A ويصل له Tag لأنه جزء من خلاصته VLAN يدور في السويتش A الذي يفرز أنه أخرجه Tag ليستطيع VLAN الانتقال لايرسل لأجهزة أخرى كـ Frame ويطلب Tag أن يخرج منه عند ثم لا يعود إليه مرة أخرى فخرج عند وصل إلى الجهاز C الذي يفرز أنه الـ Tag أنظر خلاصته بالـ VLAN وأنه ليس الجهاز رقم 8 فقط بل التالي يربطه إليه فقط وليس له جهاز آخرية وهذه هي فكرة Frame Tagging

## ٢) عملية VTP Pruning

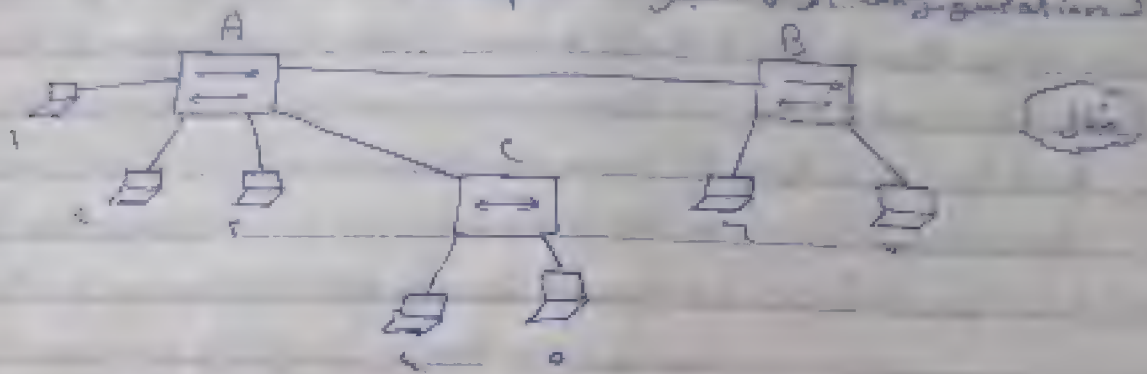
وهي خاصية تقلل عملية الـ Loop وتقوم فكرتها على أنه إذا كان جهاز يرسل إلى جهاز آخر فلا منحه مرتبط بسويتش مختلفا لكنهم تتبع VLAN مثلا في السويتش الذي له مخرج يوصلها لـ VLAN يستقبل البيانات فيها ثم لم يملك إلا أجهزة الخاصة به مرتبطه بـ VLAN وأما السويتش الذي ليس له مخرج يؤدي إلى VLAN فإنه إذا لم له تصل إليه أخرجه



فإذا المثال الجهاز (PCs) A ، B تتبع VLAN فإرسال PC1 إلى PC2 فإنه السويتشات A سيخرج من الـ Frame ينقل إلى B والجهاز B يرسلها إلى الجهاز C والجهاز D لكنه الجهاز C فقط هو الذي لديه مخرج لـ VLAN فإنه يستقبل الـ Frame فإليه D ليس لديه مخرج يوصله لـ VLAN فلا تصل إليه البيانات والجهاز C الذي استلم الـ Frame يرسلها إلى PC2 ويحاول أن يرسلها إلى السويتش F فلا يستطيع F لأنها ليس لديه مخرج يوصله بالجهاز F VLAN وبالكلام هذه الطريقة لتجنب الـ Frame من أن تكون دورا في فلا يحدث الـ Loop

## # خاصية ال Native VLAN

هذا بإختصار خاصية تقوم على حل مشكلة ال Tag في السويتشات التي لا تقبل ال configuration أمر من أجهزة ال Hub



بمجرد انه الجهاز الذي أتبع أجهزة ال Accounting وإثبات ال vlan خاصة ال Accounting وهذا vlan 50 وإذا أراد الجهاز CD مثلاً أن يرسل رسالة في الأجهزة ال Accounting فإنه يرسلها 802.1Q على ال Tag ال Frame تعمل بجهاز B هكذا وإذا لم يرسل ال vlan 50 تكتبه الجهاز C لأنه ال Hub ولا يقبل ال configuration أمر من السويتش لا يقبل ال configuration فلو وجد عليه vlan 50 ينتظر له تعلق جيب الباتة ولحل هذه المشكلة تفعل خاصية ال native vlan وهذا بإختصار أنه تلقى على ال Tag وهذا اللفظ يكون عليه ظاهرة يعني أنه عندما أقول vlan 50 ليس لها تاج فهذا أيضاً علامة أو علامة أن هذه ال vlan 50 ليس لها Tag بعد مرور الباتة إلى الجهاز C سيقراها أنها ليس لها تاج وبالتالي إذا عاد به فينتقل ويرسلها إلى الأجهزة المرتبطة به وعندما يوصلها للجهاز B سيقول أن لها تاج وهو أنه ليس لها تاج فظاهر فيستقبلها vlan 50 والتي عليها أن ترسلها لها تاج فيمر الباتة إلى أجهزة الخاصة بـ vlan 50 المتصلة به

العمل ال Native vlan تكتب تلقى سويتش ونعرف ال Native vlan

Switch 1 en

Switch # Config T

Switch (config) # int Fa 0/1

Switch (config-if) # Switch port Trunk Native vlan 50



## Allowed Vlan

# 7/5/2019

من أجل أن يكون Trunk مستطوع البورتات التي تستقبل البيانات  
 من كل VLAN فكل ما علينا فعله هو إعداد Trunk على البورتات التي  
 نريد أن تكون Trunk. ولذا نستخدم الأمر التالي في الـ Configuration  
 Switches:

Switch (config) #

Switch (config) # int Fa 0/1

Trunk البورتات

Switch (config-if) # Switchport Trunk allowed

ببورتات

① كل الـ Vlan's

Switch (config-if) # Switchport Trunk allowed All

② إضافة VLAN إلى القائمة المسموح بها

Switch (config-if) # Switchport Trunk allowed vlan add vlan id  
 10

③ إزالة الـ Vlan's من القائمة المسموح بها

Switch (config-if) # Switchport Trunk allowed vlan except 10

④ إزالة Vlan's من القائمة المسموح بها

Switch (config-if) # Switchport Trunk allowed vlan remove 5-10

# ملاحظة #

بعض السويتشات القديمة مثل بعض أجهزة ISL مفعلة بـ ISL  
 أو VLAN. فلتأكد من أن ISL أو VLAN 802.1Q هو الذي نريد استخدامه  
 كـ Vlan في الـ Vlan's. بعض السويتشات ISL مفعلة بـ ISL. فلتأكد من أن  
 Trunk مفعلة أيضاً. فلتأكد من أن ISL مفعلة أيضاً. فلتأكد من أن ISL مفعلة أيضاً.

Switch (config-if) # Switchport mode Trunk

Switch (config-if) # Switchport Trunk encapsulation dot1q

تأكد من أن المصنفات ليست قد تم حذفها من المبرمجين أو قد تم حذفها من المبرمجين

## VLAN Full Configuration

### 1] Vlan Creation

```
Switch (config) # Vlan 100 ex
```

```
Switch (config-vlan) # Name Accounting ex
```

### 2] Access port Configuration

```
Switch (config-if) # Switchport mode Access
```

```
Switch (config-if) # Switchport nonegotiate
```

```
Switch (config-if) # Switchport Access Vlan 100 ex
```

### 3] Trunk port Configuration

```
Switch (config-if) # Switchport mode Trunk
```

```
Switch (config-if) # Switchport Trunk encapsulation dot1q
```

```
Switch (config-if) # Switchport Trunk allowed vlan 10 or 20-30 ex
```

```
Switch (config-if) # Switchport Trunk native Vlan 100 ex
```

### 4] VTP Configuration

```
Switch (config) # VTP mode [server | client | transparent]
```

```
Switch (config) # VTP Domain < Name >
```

```
Switch (config) # VTP password < 123 ex >
```

```
Switch (config) # VTP pruning
```

```
Switch (config) # VTP Version. 1 or 2
```



## [5] Troubleshooting

Switch # show status

Switch # show interface [status & switchport]

Switch # show interface Trunk

Switch # show VTP status

Switch # show VTP password

## CDP - Protocol

هو بروتوكول خاص بالأجهزة سيسكو أو أنه يعمل على روترات وسويتشات سيسكو وهو اختصار لـ Cisco Discovery protocol " يعمل كما وصفنا على الأجهزة سيسكو أو أنه إذا كان هناك نوعيه مختلفيه فإنه لا يعمل

- وظيفته: - هو بروتوكول خاص بالمزامنة والمتابعة من طريقة تستطيع التعرف على جهازه السويتش وهذا البروتوكول مفيد حيث يمكنك من معرفة تصميم الشبكة من خلال معرفة الأجهزة المجاورة لكل جهاز

• الدوامر الخاصة ب CDP

[1] أمر Show CDP

Switch > en

Switch # show cdp

عند إجراء هذا الأمر ستظهر لنا المعلومات التالية:

Global CDP information:

Sending CDP packets every 60 seconds

Sending hold time value of 180 seconds

Sending CDP v2 advertisements is enabled

أولاً نلاحظ أنه `show cdp neighbors` يعرض عناوين الـ IP و MAC للجارين المباشرين فقط. هذا يعني أننا نحتاج إلى معرفة الـ IP و MAC للجارين المباشرين من أجل معرفة هويتهم الحقيقية. لذلك نستخدم الأمر `show cdp neighbors detail` الذي يعرض معلومات إضافية عن الجارين المباشرين.

في المثال التالي نلاحظ أن الأمر `show cdp neighbors detail` يعرض معلومات إضافية عن الجارين المباشرين، بما في ذلك الـ IP و MAC للجارين المباشرين، بالإضافة إلى الـ Vlan التي تنتمي إليها الـ IP و MAC للجارين المباشرين. كما نلاحظ أن الأمر `show cdp neighbors detail` يعرض معلومات إضافية عن الجارين المباشرين، بما في ذلك الـ IP و MAC للجارين المباشرين، بالإضافة إلى الـ Vlan التي تنتمي إليها الـ IP و MAC للجارين المباشرين.

في المثال التالي نلاحظ أن الأمر `show cdp neighbors detail` يعرض معلومات إضافية عن الجارين المباشرين، بما في ذلك الـ IP و MAC للجارين المباشرين، بالإضافة إلى الـ Vlan التي تنتمي إليها الـ IP و MAC للجارين المباشرين. كما نلاحظ أن الأمر `show cdp neighbors detail` يعرض معلومات إضافية عن الجارين المباشرين، بما في ذلك الـ IP و MAC للجارين المباشرين، بالإضافة إلى الـ Vlan التي تنتمي إليها الـ IP و MAC للجارين المباشرين.

📌 أمراً `show cdp neighbors`

Switch # `show cdp neighbors`

نتائج الأمر `show cdp neighbors` تظهر لنا المعلومات التالية:

Device ID	Local Interface	Holdtime	Capability	Platform
Switch1	Fa/1	180	R	2950

التي تعطينا:

- Device ID: اسم الجهاز المجاور
- Local Interface: الواجهة المحلية التي تتصل بها
- Holdtime: الوقت المتبقي حتى يتم تحديث المعلومات
- Capability: القدرات التي يمتلكها الجهاز المجاور
- Platform: منصة الجهاز المجاور

في المثال التالي نلاحظ أن الأمر `show cdp neighbors` يعرض معلومات إضافية عن الجارين المباشرين، بما في ذلك الـ IP و MAC للجارين المباشرين، بالإضافة إلى الـ Vlan التي تنتمي إليها الـ IP و MAC للجارين المباشرين. كما نلاحظ أن الأمر `show cdp neighbors` يعرض معلومات إضافية عن الجارين المباشرين، بما في ذلك الـ IP و MAC للجارين المباشرين، بالإضافة إلى الـ Vlan التي تنتمي إليها الـ IP و MAC للجارين المباشرين.



نتيجة الأمر `show cdp neighbors`



تكوين السويتش / تم

سيفر لـ 100

Device ID	local interface	Hold time	capability	platform	port ID
S1	Fa/2	180	5	1	↓
↓	↓	↓	↓	2950	Fa/1
اسم الجهاز المجاور	مخرج كابل الكاب تتصل به / أمر	زمن كاشف	سويتش	نموذج	مخرج كابل المجاور

show cdp entry switch ①  
معرفة

show cdp neighbour detail أمر ③

يقوم هذا الأمر بإظهار معلومات عن

1- IOS - نظام التشغيل

2- IP address - للجهاز المجاور

3- duplex أو half duplex للترينين ، interface : المجاورة

④ أمر منع أو تفعيل البروتوكول في إدارة تهيئة

Switch(config) # No CDP Run

تعطيله

Switch(config) # CDP Run

تفعيله وتنشيطه على بورت محدد

Switch(config) # int Fa/1

تحدد البورت

Switch(config-if) # No CDP enable

تعطيله

Switch(config-if) # CDP enable

6] أمر تعديل وقت cdp packet

Switch(config)# cdp timer 90

تعدله من 90 ثانية إلى 60 ثانية cdp packet

Switch(config)# cdp Holdtime 240

تعدله من 180 إلى 240 ثانية Holdtime

• تستطيع تغيير الوقت كما تريد والعلم من الأمر هو السابقه كمثل

7] أمر معرفة كام جالت تم ارساله واستقباله

Switch# ~~show~~ show cdp traffic

## Etherchannel

ال etherchannel هو تقنية خاصة يستطيعون تجميع جميع ما يصل إلى ثمانية لينكات  
فيزيكية physical links مع السويتش في مجموعة من Logical Link واحد وهي



مثال

فهذا المثال يوصل السويتش (S1) بالسويتش (S2) بأربعة لينكات

وكما علمنا انه بروتوكول STP يقوم بتفعيل لينك واحد فقط واعتبار الباقى كإضافي

فما هو الفرق بين تفعيل أكثر من لينك لتجميع عمل في الـ (LACP)

أقول ان الـ **etherchannel** هو اعتبار هذه اللينكات الأربعه كإنه مكان المثال كأنه لينك واحد  
ولا استفادة منك انك انجز لينك واحد



## غرائدها

### 1- زيادة ال Bandwidth

لذا نقول أنه هيك التوافق هو ما يجعلنا نركب حواشي استطيع أو استطيع  
بم أن نظامنا هو الذي يتم حيث أن كل واحد يمكنه هو الذي تمت من (الاستطيعات)  
ما استطيع ال - استطاعة لـ  $2 \times 10$  حواشي رتابة

2- استقرار النقل في حالة انقطاع الحبل  $\rightarrow$  Redundancy  
إذا كان لدينا في ال Bandwidth 10 لينكات فلو انقطع أحدها فإننا لن نفقد شيئاً منهم  
فيطيعون نقل البيانات معه تأخر بالقليل (الثاني)

### 3- تقوم بال Load Balancing

حيث تقوم بتوزيع ال Frame على اللينكات بشكل متساوٍ فلو ما نقل ال الخط  
على كامل حواشي فقط .

### 4- زيادة الحواشي Access

## شروطها

- 1- أن تكون جميع الحواشي متصلة  $\rightarrow$  Full Mesh
- 2- أن يكون كل ال Bundle جزءاً من ال لينكات وجميعها  $\rightarrow$  C
- 3- أن يكون بين كل سريرتين ال Bundle 2 جزءاً من ال التوجيه الباسل  
الثاني سنعمل  $\rightarrow$  Redundancy إذا كان بين حواشي  $2 \times 10$  سيوفها  
العمل إذا ما حاله تلف ال ال Bundle الأول .
- 4- كل الحواشي في ال Bundle لا بد أن تكون في نفس السريرتين و Duplex mode

## العداد ال Etherchannel

### Manual Bundling

### Automatic Bundling

تلك العداد ال ether channel

## Manual Bundling [1]

هذه الطريقة هي الطريقة التي نستخدمها في البداية

Switch(Config) # int Fa/1

أو

Switch(Config) # int range Fa/1-3

Switch(Config-if) # channel-group 1 mode on

ونذهب للسويتش الآخر ونعمل نفس الخطوات ونأكد أنه mode on في الثانية  
الأخرى، هويتش الآخر؟

## Automatic Bundling [2]

هذه الطريقة هي الطريقة الأوتوماتيكية



LACP

"قياس مدع مع حثو ونفقا"

PAgP

"خاصة بـ PAgP"

"Desirable - Auto"

لا يوجد فرق في العمل بين البروتوكولين إلا الأجهزة التي تدعمها كـ PAgP

إذا استخدمنا أحد البروتوكولين سيعمل لا بد أنه نستخدمه في السويتش الآخر

PAgP [3]

Switch(Config) # int range Fa/1-3

Switch(Config-if) # switchport mode trunk

Switch(Config-if) # ~~channel-group~~ channel-protocol PAgP

Switch(Config-if-range) # channel-group 1 mode desirable

نبدأ العمل desirable كـ PAgP في الثانية، "Desirable أو Auto"

Switch(Config-if-range) # No Shutdown

Switch(Config-if-range) exit.



Lesson 5

Switch (Config) # int range 1/24

Switch (Config-if-range) # ~~channel~~ Switchport mode Trunk

Switch (Config-if-range) # Channel-protocol LACP

Switch (Config-if-range) # channel-group 1 mode active

Switch (Config-if-range) # no shutdown

Switch (Config-if-range) # exit

passive , Active  $\rightarrow$  Active  $\rightarrow$  Active  $\rightarrow$  Active  $\rightarrow$  Active

\* modes \* أحوال الحود \*

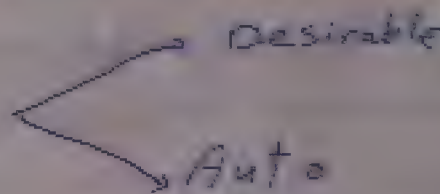
Switch

أحوال الـ mode قبل الـ etherchannel :  $\rightarrow$  mode on

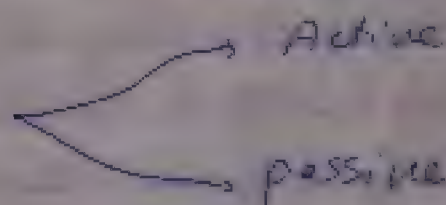
① mode on

mode on

② mode Desirable



③ mode Active



④ mode Auto

$\rightarrow$  mode Desirable

\* أرقام الـ Show : etherchannel :  $\rightarrow$  Show

Switch # show etherchannel

Switch # show ether channel port-channel

Switch # show ether channel Summary

Switch # show ip interface brief





## Remote Access

وهنا سنناقش طريقة الدخول الى اعدادات السويتش لكي نخرج  
الى Console وناستلم برنامج Hyper Term او برنامج  
للدخول الى السويتش وبهذه الطريقة ال Configuration

هناك طريقة اخرى لها طريقة الدخول عن بعد ان هذه طريقة جهاز من أجهزة  
الشبكات عليه الدخول الى اعدادات السويتش ولكنه ليس كما نبدأ ان نرى توضيحها.

عليه انه يتم التحكم من السويتش عن بعد اما عن طريق SSH او عن طريق  
Telnet

### البيانات ال Remote Access

- ① اعداد IP للسويتش
- ② تفعيل ال Remote Access ووضع باسورد
- ③ عمل password على privileged mode
- ④ اعداد IP للراوتر " Get way "

### 1 اعداد مع IP للسويتش

من البداية السويتش لا يتقبل ب IP لكن المصنوع الذي استطع انه  
أقبل عليه IP هو ال L/an  
الجهاز الذي يستطيع الدخول به هو الجهاز المشترك مع ال L/an الذي  
نفذ IP ويكون له نفس العنوان للشبكة " Subnet mask "

# او من السويتش لاعداد IP

Switch > en

Switch # config ?

Switch # conf t

Switch(Config-if) # no shutdown

Switch(Config-if) # IP address 192.168.1.1 255.255.255.0

Switch(Config-if) # exit

تغيير الـ interface name

تغيير الـ interface description

الخطوات الـ 1 و 2 و 3 و 4 و 5 و 6 و 7 و 8 و 9 و 10 و 11 و 12 و 13 و 14 و 15 و 16 و 17 و 18 و 19 و 20 و 21 و 22 و 23 و 24 و 25 و 26 و 27 و 28 و 29 و 30 و 31 و 32 و 33 و 34 و 35 و 36 و 37 و 38 و 39 و 40 و 41 و 42 و 43 و 44 و 45 و 46 و 47 و 48 و 49 و 50 و 51 و 52 و 53 و 54 و 55 و 56 و 57 و 58 و 59 و 60 و 61 و 62 و 63 و 64 و 65 و 66 و 67 و 68 و 69 و 70 و 71 و 72 و 73 و 74 و 75 و 76 و 77 و 78 و 79 و 80 و 81 و 82 و 83 و 84 و 85 و 86 و 87 و 88 و 89 و 90 و 91 و 92 و 93 و 94 و 95 و 96 و 97 و 98 و 99 و 100 و 101 و 102 و 103 و 104 و 105 و 106 و 107 و 108 و 109 و 110 و 111 و 112 و 113 و 114 و 115 و 116 و 117 و 118 و 119 و 120 و 121 و 122 و 123 و 124 و 125 و 126 و 127 و 128 و 129 و 130 و 131 و 132 و 133 و 134 و 135 و 136 و 137 و 138 و 139 و 140 و 141 و 142 و 143 و 144 و 145 و 146 و 147 و 148 و 149 و 150 و 151 و 152 و 153 و 154 و 155 و 156 و 157 و 158 و 159 و 160 و 161 و 162 و 163 و 164 و 165 و 166 و 167 و 168 و 169 و 170 و 171 و 172 و 173 و 174 و 175 و 176 و 177 و 178 و 179 و 180 و 181 و 182 و 183 و 184 و 185 و 186 و 187 و 188 و 189 و 190 و 191 و 192 و 193 و 194 و 195 و 196 و 197 و 198 و 199 و 200 و 201 و 202 و 203 و 204 و 205 و 206 و 207 و 208 و 209 و 210 و 211 و 212 و 213 و 214 و 215 و 216 و 217 و 218 و 219 و 220 و 221 و 222 و 223 و 224 و 225 و 226 و 227 و 228 و 229 و 230 و 231 و 232 و 233 و 234 و 235 و 236 و 237 و 238 و 239 و 240 و 241 و 242 و 243 و 244 و 245 و 246 و 247 و 248 و 249 و 250 و 251 و 252 و 253 و 254 و 255 و 256 و 257 و 258 و 259 و 260 و 261 و 262 و 263 و 264 و 265 و 266 و 267 و 268 و 269 و 270 و 271 و 272 و 273 و 274 و 275 و 276 و 277 و 278 و 279 و 280 و 281 و 282 و 283 و 284 و 285 و 286 و 287 و 288 و 289 و 290 و 291 و 292 و 293 و 294 و 295 و 296 و 297 و 298 و 299 و 300 و 301 و 302 و 303 و 304 و 305 و 306 و 307 و 308 و 309 و 310 و 311 و 312 و 313 و 314 و 315 و 316 و 317 و 318 و 319 و 320 و 321 و 322 و 323 و 324 و 325 و 326 و 327 و 328 و 329 و 330 و 331 و 332 و 333 و 334 و 335 و 336 و 337 و 338 و 339 و 340 و 341 و 342 و 343 و 344 و 345 و 346 و 347 و 348 و 349 و 350 و 351 و 352 و 353 و 354 و 355 و 356 و 357 و 358 و 359 و 360 و 361 و 362 و 363 و 364 و 365 و 366 و 367 و 368 و 369 و 370 و 371 و 372 و 373 و 374 و 375 و 376 و 377 و 378 و 379 و 380 و 381 و 382 و 383 و 384 و 385 و 386 و 387 و 388 و 389 و 390 و 391 و 392 و 393 و 394 و 395 و 396 و 397 و 398 و 399 و 400 و 401 و 402 و 403 و 404 و 405 و 406 و 407 و 408 و 409 و 410 و 411 و 412 و 413 و 414 و 415 و 416 و 417 و 418 و 419 و 420 و 421 و 422 و 423 و 424 و 425 و 426 و 427 و 428 و 429 و 430 و 431 و 432 و 433 و 434 و 435 و 436 و 437 و 438 و 439 و 440 و 441 و 442 و 443 و 444 و 445 و 446 و 447 و 448 و 449 و 450 و 451 و 452 و 453 و 454 و 455 و 456 و 457 و 458 و 459 و 460 و 461 و 462 و 463 و 464 و 465 و 466 و 467 و 468 و 469 و 470 و 471 و 472 و 473 و 474 و 475 و 476 و 477 و 478 و 479 و 480 و 481 و 482 و 483 و 484 و 485 و 486 و 487 و 488 و 489 و 490 و 491 و 492 و 493 و 494 و 495 و 496 و 497 و 498 و 499 و 500 و 501 و 502 و 503 و 504 و 505 و 506 و 507 و 508 و 509 و 510 و 511 و 512 و 513 و 514 و 515 و 516 و 517 و 518 و 519 و 520 و 521 و 522 و 523 و 524 و 525 و 526 و 527 و 528 و 529 و 530 و 531 و 532 و 533 و 534 و 535 و 536 و 537 و 538 و 539 و 540 و 541 و 542 و 543 و 544 و 545 و 546 و 547 و 548 و 549 و 550 و 551 و 552 و 553 و 554 و 555 و 556 و 557 و 558 و 559 و 560 و 561 و 562 و 563 و 564 و 565 و 566 و 567 و 568 و 569 و 570 و 571 و 572 و 573 و 574 و 575 و 576 و 577 و 578 و 579 و 580 و 581 و 582 و 583 و 584 و 585 و 586 و 587 و 588 و 589 و 590 و 591 و 592 و 593 و 594 و 595 و 596 و 597 و 598 و 599 و 600 و 601 و 602 و 603 و 604 و 605 و 606 و 607 و 608 و 609 و 610 و 611 و 612 و 613 و 614 و 615 و 616 و 617 و 618 و 619 و 620 و 621 و 622 و 623 و 624 و 625 و 626 و 627 و 628 و 629 و 630 و 631 و 632 و 633 و 634 و 635 و 636 و 637 و 638 و 639 و 640 و 641 و 642 و 643 و 644 و 645 و 646 و 647 و 648 و 649 و 650 و 651 و 652 و 653 و 654 و 655 و 656 و 657 و 658 و 659 و 660 و 661 و 662 و 663 و 664 و 665 و 666 و 667 و 668 و 669 و 670 و 671 و 672 و 673 و 674 و 675 و 676 و 677 و 678 و 679 و 680 و 681 و 682 و 683 و 684 و 685 و 686 و 687 و 688 و 689 و 690 و 691 و 692 و 693 و 694 و 695 و 696 و 697 و 698 و 699 و 700 و 701 و 702 و 703 و 704 و 705 و 706 و 707 و 708 و 709 و 710 و 711 و 712 و 713 و 714 و 715 و 716 و 717 و 718 و 719 و 720 و 721 و 722 و 723 و 724 و 725 و 726 و 727 و 728 و 729 و 730 و 731 و 732 و 733 و 734 و 735 و 736 و 737 و 738 و 739 و 740 و 741 و 742 و 743 و 744 و 745 و 746 و 747 و 748 و 749 و 750 و 751 و 752 و 753 و 754 و 755 و 756 و 757 و 758 و 759 و 760 و 761 و 762 و 763 و 764 و 765 و 766 و 767 و 768 و 769 و 770 و 771 و 772 و 773 و 774 و 775 و 776 و 777 و 778 و 779 و 780 و 781 و 782 و 783 و 784 و 785 و 786 و 787 و 788 و 789 و 790 و 791 و 792 و 793 و 794 و 795 و 796 و 797 و 798 و 799 و 800 و 801 و 802 و 803 و 804 و 805 و 806 و 807 و 808 و 809 و 810 و 811 و 812 و 813 و 814 و 815 و 816 و 817 و 818 و 819 و 820 و 821 و 822 و 823 و 824 و 825 و 826 و 827 و 828 و 829 و 830 و 831 و 832 و 833 و 834 و 835 و 836 و 837 و 838 و 839 و 840 و 841 و 842 و 843 و 844 و 845 و 846 و 847 و 848 و 849 و 850 و 851 و 852 و 853 و 854 و 855 و 856 و 857 و 858 و 859 و 860 و 861 و 862 و 863 و 864 و 865 و 866 و 867 و 868 و 869 و 870 و 871 و 872 و 873 و 874 و 875 و 876 و 877 و 878 و 879 و 880 و 881 و 882 و 883 و 884 و 885 و 886 و 887 و 888 و 889 و 890 و 891 و 892 و 893 و 894 و 895 و 896 و 897 و 898 و 899 و 900 و 901 و 902 و 903 و 904 و 905 و 906 و 907 و 908 و 909 و 910 و 911 و 912 و 913 و 914 و 915 و 916 و 917 و 918 و 919 و 920 و 921 و 922 و 923 و 924 و 925 و 926 و 927 و 928 و 929 و 930 و 931 و 932 و 933 و 934 و 935 و 936 و 937 و 938 و 939 و 940 و 941 و 942 و 943 و 944 و 945 و 946 و 947 و 948 و 949 و 950 و 951 و 952 و 953 و 954 و 955 و 956 و 957 و 958 و 959 و 960 و 961 و 962 و 963 و 964 و 965 و 966 و 967 و 968 و 969 و 970 و 971 و 972 و 973 و 974 و 975 و 976 و 977 و 978 و 979 و 980 و 981 و 982 و 983 و 984 و 985 و 986 و 987 و 988 و 989 و 990 و 991 و 992 و 993 و 994 و 995 و 996 و 997 و 998 و 999 و 1000

5. تفعيل الـ Remote

لو عملنا أمر Show Run على السويتش -- يظهر لنا

Line Con -- Console

Line vty 0 4 -- مضافا اليه هناك 5 أجهزة تستطيع الدخول والتحكم في السويتش

# اواخر السويتش

Switch > en

Switch # Config T

Switch(Config) # Line vty 0 4

Switch(Config-line) # password 123

Switch(Config-line) # login

Switch(Config-line) # exit

تغيير الـ password

السويتش الـ 123

5. عمل password على الـ privileged mode

Switch(Config) # enable secret 123

Switch(Config) # enable password 123

لأن الـ 123 هي كلمة المرور



# الطريقة البديلة أيضا إصدار Remote Access  
للمسؤول عن طريق برنامج الوصول Telnat SSH

### الطريقة الـ Telnat

نحتاج إلى جهاز رقم ٢٢ الذي نريد منه محاولة الوصول والتحكم في السويتش

١- عند تشغيل start ونفاز Run نكتب الأمر

٢- عند الوصول نضع End نكتب الأمر Telnat كالتالي

Telnat 192.10.10.1

أو إذا كنا نكتب Telnat نكتب الـ IP الخاص بالسويتش الذي نريد الاتصال به

عندما نتقن الوصول والتحكم في السويتش نكتب الـ password

هذه الطريقة الـ Telnat طريقة غير آمنة حيث يتم إرسال البيانات دونه  
تشفير فيستطيع المهاجم باستخدام برامج Sniffing أن يستغيب البيانات  
الخاصة بـ IP الجهاز الذي نريد الاتصال به الـ password وبالتالي التحكم في  
السويتش.

٣- نستخدم الـ Telnat البورت رقم ٢٣.

### الطريقة الـ SSH

هذه طريقة أخرى للاتصال بجهاز السويتش تتميز بأنها آمنة حيث طريقة الـ Telnat  
حيث أنها لا تملك التشفير والـ SSH هي اختصار لـ "Secure Shell"  
وتستخدم لهذا الغرض بروتوكول البورت ٢٢

٤- خطوات استخدام الـ

١- الاسم الذي نريد الاتصال به الـ Default السويتش

٢- اسم الـ username { password

٣- اسم الـ Domainname يكون عبارة عن اسم الجهاز الأبعد الذي نريد الاتصال به

# Ahmed Config # 3211

Switch # en

Switch(Config)#

في غير اسم المستخدم

Switch(Config)# Host Ahmed

الاسم المستخدم

password { username

Switch(Config)# username Tarek Secret 1234

Domain name

Switch(Config)# Ip Domainname Egypt.com

وتكون الـ domain ينتهي بـ .com أو .org أو .net

① تفعيل التشفير - لا بد من تغيير اسم المستخدم

~~Switch~~ Ahmed(Config)# crypto key generate rsa

لأننا نلزم أن يكون اسم الـ اسماء الخاصة بـ SSH والاسماء تكون مسفرة

② تمديد الـ داخل عن طريق Remote وواجهة الـ استخدام SSH

Ahmed(Config)# Line vty 0 4

الأجهزة التي سوف نقوم بـ Remote

Ahmed(Config-line)# Transport input ssh

استخدام الـ SSH فقط

Ahmed(Config-line)# login local

الآن الأضيق الخلف الدخول للموسيقى باستخدام SSH إلا أنه طريقة الـ LAN الـ الدخول

الممكنة فعلاً بالموسيقى وعدم السماح بـ الـ خارج الـ LAN بالدخول من مسبقاً

من البيت عن طريق الـ الإنترنت



طريقة بسيطة

- 1- إنشاء user SSH على switch
- 2- إعدادات Firewall
- 3- إعدادات Router

SSH - L username jf switch

أو اسم المودم

SSH - L Tarek 192.16.16.1

عندما يطلب اسم المودم

password : 1234

فيجب كتابة اسم المودم بالأسفل privileged exec

20 هذه الطريقة خاصة ببرنامج Packet Tracer

كيفية الحقيقة من برنامج Putty

1- اختيار الاتصال SSH

2- كتابة IP الجهاز السويش

3- اختيار open

بعد فتح النافذة التالية نضع كتاب الأوامر عليها

# أوامر SSH كاملة

```
Switch(Config) # host S1
S1(Config) # username Ahmed secret 1234
S1(Config) # Ip Domain-name 192.16.16.1
S1(Config) # Line vty 0 4
S1(Config-line) # Transport input SSH
S1(Config-line) # login local
S1(Config-line) # exit
```

## # إعدادات الـ Configuration

تتميز هذه الإعدادات بأنها ليست ثابتة بل يمكن تغييرها في أي وقت أثناء تشغيل الجهاز. كما أنها لا تخزن في الـ RAM بل في الـ NVRam. لذلك فإنها تبقى موجودة حتى بعد إغلاق الجهاز وإعادة تشغيله. كما أنها لا تتغير مع تحديث البرنامج.

Switch # Copy Run start

نقل الـ Config من الـ NVRam

نقل الـ Config من الـ NVRam

(RAM) هي ذاكرة يتم تخزين البرامج والبيانات فيها. وهي سريعة ولكنها مؤقتة. عند إيقاف الجهاز، يتم تخزين البيانات في الـ NVRam. عند إعادة التشغيل، يتم تحميل البيانات من الـ NVRam إلى الـ RAM.

(NVRam) هي ذاكرة يتم تخزين البرامج والبيانات فيها. وهي سريعة ولكنها مؤقتة. عند إيقاف الجهاز، يتم تخزين البيانات في الـ NVRam. عند إعادة التشغيل، يتم تحميل البيانات من الـ NVRam إلى الـ RAM.

(Flash memory) هي ذاكرة يتم تخزين البرامج والبيانات فيها. وهي سريعة ولكنها مؤقتة. عند إيقاف الجهاز، يتم تخزين البيانات في الـ NVRam. عند إعادة التشغيل، يتم تحميل البيانات من الـ NVRam إلى الـ RAM.

# أزرار Copy

Switch # Copy Run start

نقل الـ Config من الـ NVRam

Switch # erase start

نقل الـ Config من الـ NVRam



## # مفاهيم عامة #

### Broadcast [II]

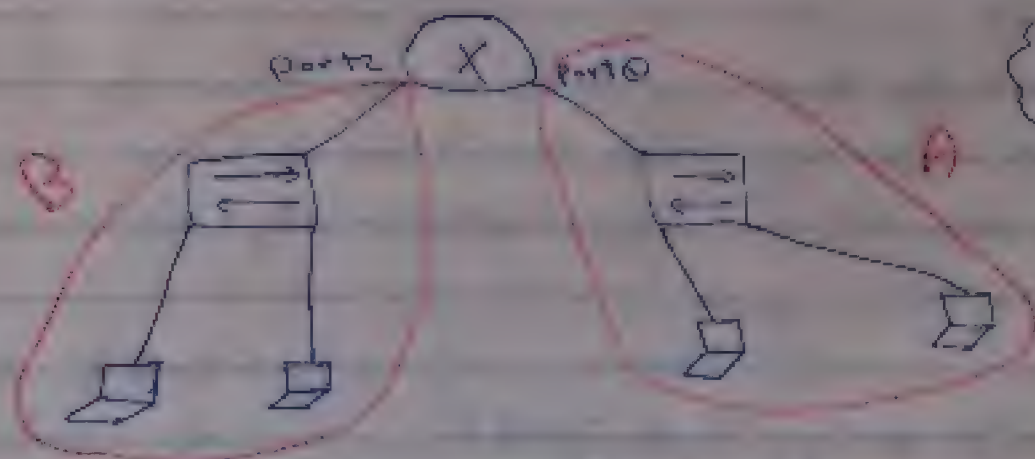
هو عملية إرسال البيانات إلى جميع الـ Hosts الموجودة على الشبكة  
ويجب معرفة أنه لكل شبكة Broadcast address خاص بها

مثال

إذا كان لدينا شبكة عنواني  $10.0.0.0/8$  فإن Broadcast address لهذه  
الشبكة هو  $10.255.255.255$  أي أن Broadcast address هو عنوان الـ IP  
الأخير من الشبكة الذي يتم تمريره إلى جميع الـ Hosts

### Broadcast domain [C]

كلما ذكرنا فإنه يشير إلى Broadcast domain فمثلاً داخل الشبكة الواحدة لذلك  
Broadcast domain "نطاق البث" هو عند حدود حصرية هذه الشبكة



فما هذا الشكل لدينا شبكتيه كل شبكة عبارة عن الموترين وأجهزة الـ PC  
متصلة ببعضها في الراوتر

[A] الشكل A هو Broadcast domain لهذه الشبكة

[B] الشكل B هو Broadcast domain لهذه الشبكة

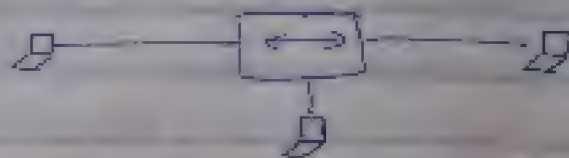
## Collision domain [3]

المنطقة Collision domain هي المنطقة التي تقع ضمنها جميع أجهزة الشبكة التي تتصل مع بعضها البعض.

أو Collision domain هي المنطقة التي

أو Collision domain هي المنطقة التي تتصل مع بعضها البعض.

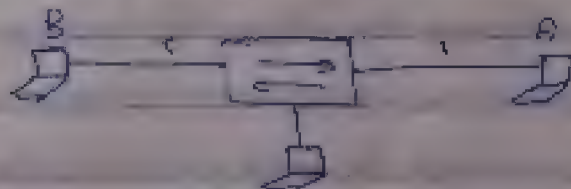
مثال



في هذا المثال لدينا جهاز Hub وكرتبه أجهزة PC وال Hub من أجهزة Layer 2  
 وهو لا يستطيع التفرقة على IP أو ال mac address لذلك فإنه يرسل البيانات لكل الأجهزة  
 المتصلة به ك Broadcast. أي أن جميع الأجهزة التي تتصل بها الجهاز تتلقى الرسالة سواء كانت مخصصة  
 له أم لا. فإذا حدث أن أرسل جهاز ما رسالة أو أكثر من تلك التي يجب أن تصل إلى Hub فكلها  
 ال Hub يأخذها كلها ولا يرسلها إلا إلى الجهاز الذي أرسلها. فكل هذه الحالة هي حالة  
 تصادم للبيانات Collision domain. فجميع تقنيات ال Hub

المثال الثاني: شبكة تتصل بال Hub بسويتش

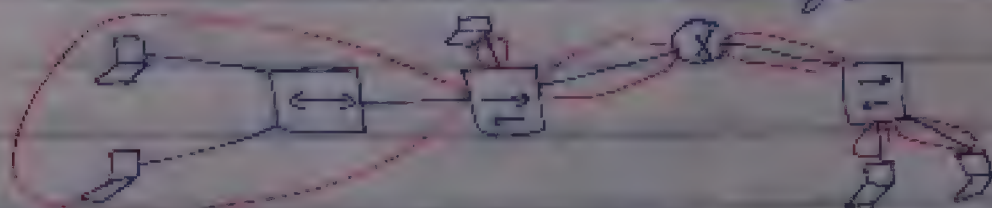
مثال 2



السويتش من أجهزة Layer 2 أي أنه يفصل ال mac address وبالتالي فإنه يوجه البيانات  
 تجاه الجهاز الصحيح مباشرة. فكل رسالة لها عنوانها الخاص. وهذا يعني أنه التصادم لم يحدث هنا  
 كل تقنيات السويتش بل في حالة واحدة فقط وهو إذا أراد الجهاز A مثلاً إرسال  
 رسالة إلى B مثلاً B يرسل الرسالة إلى A فحدث تصادم. فكلما كان الأول أو الثاني حسب  
 مكان تصادم البيانات، نستخلص منه ذلك أن

Collision Domain هو الكمية التي يقع فيها جميع أجهزة الشبكة التي تتصل مع بعضها البعض.

مثال



كل تقنيات السويتش اعتبرت كل واحدة من Collision domain. وذلك لأن السويتش يفرق بين الراوتر والسويتش  
 ال Hub السويتش وتفرقاته كاملة Collision domain. لأنه يرسل البيانات Broadcast فكل جهاز التصادم



## ملخص على الأوامر الأساسية

### [1] Switch Modes

Switch > enable	→	user mode
Switch #	→	privileged mode
Switch (config) #	→	Global mode
Switch (config-if) #	→	Interface mode
Switch (config-subif) #	→	Subinterface mode
Switch (config-line) #	→	Line mode

### [2] Help Commands

Switch > ?	show list help Command
------------	------------------------

### [3] Show Commands

Switch # show version	Software & hardware info
Switch # show flash	Flash memory info
Switch # show mac-address-table	
Switch # show running-config	Config. in Ram
Switch # show startup-config	Config. in NVRam
Switch # show vlan	Vlan Configuration
Switch # show interfaces	Interface information
Switch # show spanning-tree	STP information
Switch # show vtp status	VTP info.
Switch # show cdp neighbors	list of CDP neighbors
Switch # show cdp neighbors detail	more info about neighbors

Switch # show ip interface brief  
Switch # show etherchannel

Switch # show etherchannel

### [4] Reset Switch Config.

- ① Switch # delete flash : vlan.dat  
Delete Filename [vlan.dat]? (enter) → yes  
Delete Flash vlan.dat? confirm (enter)
- ② Switch # erase startup-config
- ③ Switch # Reload

### [5] To Set hostname

Switch # config T

Switch (config) # hostname S<sub>1</sub> or host S<sub>1</sub>

S<sub>1</sub> (config) # exit

### [6] To Set password

#### A - privileged mode

Switch (config) # enable password S<sub>1</sub> ... سریع

Switch (config) # enable secret S<sub>2</sub> ... مطمئن

Switch (config) # service password-encryption تشفیر رمز عبور

#### B - Console mode

Switch (config) # line console 0

Switch (config-line) # password S<sub>3</sub> ...

Switch (config-line) # login

Switch (config-line) # exit



## C - vTy mode

Switch (config) # line vTy ex  
Switch (config-line) # password ex  
Switch (config-line) # login  
Switch (config-line) # exit

## [7] Speed and Duplex

Switch (config) # int Fa ex  
Switch (config-if) # duplex half or Full or Auto  
Switch (config-if) # speed 10 or 100 or Auto

## [8] port Security

Switch (config) # int Fa ex  
Switch (config-if) # switchport mode Access  
Switch (config-if) # switchport port-security  
Switch (config-if) # switchport port-security mac-address ex

[or] Switch (config-if) # switchport port-security mac-address sticky

Switch (config-if) # switchport port-security maximum ?

Switch (config-if) # switchport port-security mac-address ex

Switch (config-if) # switchport port-security violation shutdown or protect or restrict

Switch (config-if) # exit

Switch (config) # exit

Switch # show port-security address

## 9) STP

① تكوين جدار الحماية

Switch(Config) # spanning-tree vlan ex Root primary

② التحويل إلى Rapid-pvst

• التحويل إلى Rapid-pvst

Switch(Config) # int Fa / ex ---

Switch(Config-if) # spanning-tree port fast

• التحويل إلى Rapid-pvst

Switch(Config) # spanning-tree mode Rapid-pvst

Switch # show spanning-tree

## 10) VLAN

### 1. Creation vlan

Switch(Config) # vlan ex

Switch(Config-vlan) # Name ex

### 2. Access port Config.

Switch(Config-if) # switchport mode Access

Switch(Config-if) # switchport nonegotiate

Switch(Config-if) # switchport Access vlan ex

### 3. Trunk ports Config.

Switch(Config-if) # switchport mode Trunk

Switch(Config-if) # Switchport Trunk encapsulation dot1q

Switch(Config-if) # Switchport Trunk allowed vlan ex

Switch(Config-if) # Switchport Trunk native vlan ex



## 11 VTP

Switch (config) # vtp mode [server - client - transparent]  
Switch (config) # vtp domain ex  
Switch (config) # vtp password ex  
Switch (config) # vtp pruning  
Switch (config) # vtp version  
Switch # show vtp status  
Switch # vtp password

## 12 CDP

Switch # show cdp neighbors  
Switch # show cdp neighbors details  
Switch (config) # CDP Run تنشيطه  
Switch (config) # No cdp Run تعطيله  
Switch (config-if) # CDP enable تنشيطه لـ بور  
Switch (config-if) # No cdp enable تعطيله لـ بور  
Switch (config) # Cdp timer ex تغيير وقت cdp packet  
Switch (config) # Cdp Hold time ex تغيير الـ Hold time  
Switch # show cdp Traffic معرفة تاكيد انتم قماره واستقباله

## 13 Ether channel

① manual

Switch (config) # int f0/ ex  
Switch (config-if) # channel-group 1 mode on  
وتعمل 30 اخره السوفيشي الآخر

## ① Automatic

Switch(config) # int Fa/...

Switch(config-if) # Switchport mode Trunk

Switch(config-if) # channel-protocol Pagp Pagp default

Switch(config-if) # channel-protocol Lacp Lacp default

Switch(config-if) # channel-group 1 mode desirable (pagp)

Switch(config-if) # channel-group 1 mode Active (Lacp)

Switch(config-if) # no shutdown

Switch(config-if) # exit

Switch # show etherchannel

Switch # show etherchannel summary

Switch # show etherchannel port-channel

## ② Remote Access

① إعداد الـ IP

Switch(config) # int vlan 1

Switch(config-if) # no shutdown

Switch(config-if) # Ip address Ex 10.1.1.0 255.0.0.0

Switch(config-if) # exit

② إعداد الـ password

Switch(config) # line vty 0

Switch(config-line) # password ex

Switch(config-line) # login

Switch(config-line) # exit

③ إعداد الـ privileged password

Switch(config) # enable password ex

or Switch(config) # enable secret ex



## 15) SSH

Switch(config) # host S1 تقريباً

Switch(config) # username ex Secret ex اسم المستخدم وكلمة المرور

Switch(config) # Ip Domain-name ex.com

S1(config) # Crypto Key generate rsa تفعيل التشفير والبدء بتغيير التشفير

# تمديد الداخل SSH فقط

S1(config) # line vty 0 4

S1(config-line) # Transport input SSH

S1(config-line) # login local

منع الدخول، الاسم LAN

S1(config-line) # exit

# IP Subnetting

تعريف Subnet IP

هو عبارة عن تقسيم شبكة على الشبكة بحيث يصبح عنوان خاص بالقطاع لا يتشارك مع جهاز آخر على الشبكة فيعمل هذا العنوان الوصول للجهاز ويسمح له بالاتصال بشبكة الأجهزة.

شكل الـ IP

يتكون الـ IP من 4 خانات تسمى octet يفصل بينها 3 octet وآخر علامة عشرية [dot] كما يظهر المثال IP 192.168.1.10  
كل octet مكون من 8 Bit والـ 8 Bit عبارة عن رقم وله قيمة واحدة أو صفر أي أن الـ octet مكون من 8 وحدات أو 8 أرقام أو 8 وحدات أصغر  
بالنسبة الـ IP  $32 \text{ Bit} = 4 \times \text{octet}$  حيث أن  $4 \times \text{octet} = 32 \text{ Bit}$   

$$32 \text{ Bit} = 4 \times 8 \text{ Bit} = \text{IP}$$

$$32 \text{ Bit} = \text{IP}$$

يتم كتابة الـ IP بأحدى الطريقتين

- 1- باستخدام النظام العشري "Decimal" مثال 10.1.1.2
- 2- باستخدام النظام الثنائي "Binary" مثال 11111111.11111111.11111111.11111111

وهو ثنائي لأنه لا يستخدم إلا الواحد والصفر

- 3- باستخدام النظام الستاسي عشرى "hexadecimal" مثال AC10IE38

هذا النظام الأضيق يستخدم في سجل النظام Windows Registry  
والطبع أكثرهم استخداماً هو باستخدام النظام العشري مثل 10.1.1.2



## # عنوان الشبكة Network address

هو عنوان يستخدم لإرسال البيانات إلى شبكة محددة عليه. ومن الأمثلة عليه 10.0.0.0 172.16.0.0 192.168.10.0

## # Broadcast address

هو العنوان الذي يستخدمه كل الأجهزة والمعدات لإرسال معلومات لجميع الأجهزة على الشبكة. ومن الأمثلة عليه 255.255.255.255 والذي يقوم بإرسال بيانات لجميع أجهزة الشبكة. مثال آخر 172.16.255.255 هو Broadcast للشبكة 172.16.0.0 وكذلك 192.168.10.255 هو Broadcast للعنوان 192.168.10.0

# هذه العنوانان الـ Broadcast و Network لا يتحصل عليهما أي جهاز في الشبكة. كلمة ما فيها هو العنصر الوحيد المتأصلة لأجهزة الشبكة وكل جهاز رئيسي Host ويكون له عنوان غير الأخير لأنه تأخذ مستقر كونه نفس الشبكة.

مثال: الجهاز A له IP = 10.24.0.1 والجهاز الثاني له 10.24.0.2

فهذا له عنوان هو الأخير له عنوان

مثال آخر: جهاز له IP 192.168.1.2 والآخر 192.168.1.3 نلاحظ

أنهما يشتركان في نفس عنوان الشبكة وهو (192.168.1) كلمة آخرهما عنوان كل منهما فالأول هو الثاني

## # مفهوم Subnetmask

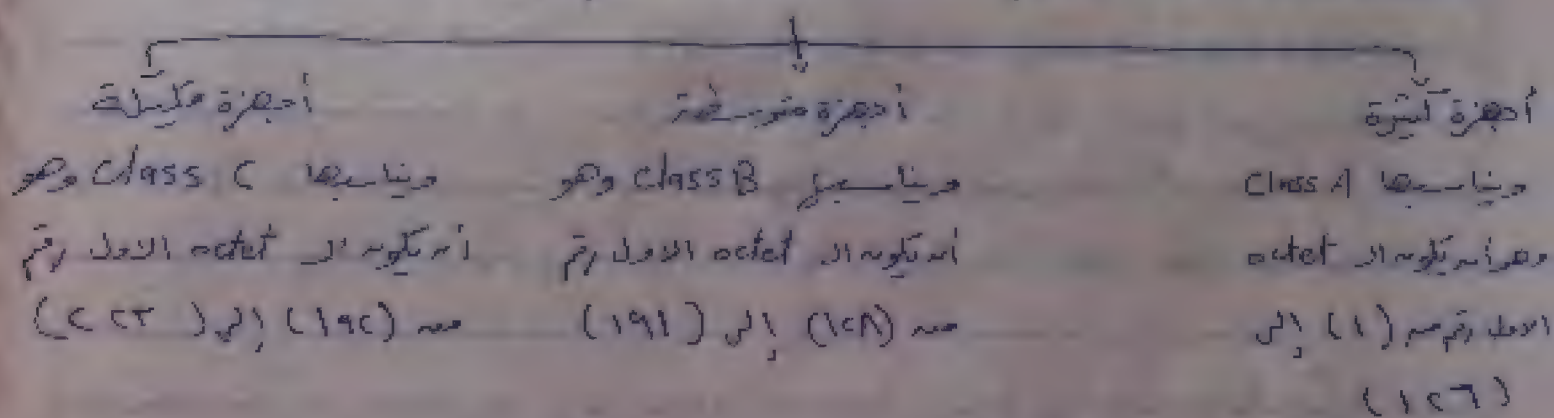
هو رقم يتلوه أيضًا Bit مخصصة أيضًا إلى 1 أو 0 يكون هذا الرقم مراقبًا للـ IP و Subnetmask هي معلومات حول الشبكة التي ينتمي إليها IP address. بمعنى معرفة عنوان الشبكة سواء كانت رئيسية أو فرعية ومنه يمكن معرفة عدد العنود الممكنة في هذه الشبكة.

أي شبكة أهر ما يجب مراعاة كتابتها بصورة سليمة هو الـ IP address والـ Subnetmask

من حيث كفاءة IP على جهاز كمبيوتر يقوم ذلك العمل كإضافة إلى Subnet mask بصورة تلقائية

في IP كل فرقة يتكون من 4 octets وكل octet يتكون من رقم من 0 إلى 255  
معنى IP - 255 اختصار لكل octet رقم من 0 إلى 255 وهذا الصورة فلسفة تسمى  
بشكل التفصيل.

فكرة إذا كتبنا IP عنواني لكل جهاز من أجهزة الشبكة فسيظهر ذلك إلى أن هناك  
الفرقة من صانعة الشبكة ومعرفة أماكن الأجهزة في الشبكة من شبكة ما مثلاً  
لذلك قامت منظمات شهيرة بإيجاد حل لمشكلة العنونة هذه وتلك  
المنظمة هي منظمة IANA [Internet Assigned Number Authority]  
قامت هذه المنظمة بتقسيم الشبكات حسب الحجم إلى ثلاث أنواع



بالإضافة إلى Class D من (224) إلى (239)  
Class E من (240) إلى (255)

رقم 127 يتم إدراجه لأنه مخصص للـ Troubleshooting  
فيلو السائل الشرائح لجميع الـ Classes مع الـ Subnet mask

class	Range	BeFault mask	Hosts
A	1 - 126	255.0.0.0	16,777,774
B	128 - 191	255.255.0.0	65,534
C	192 - 223	255.255.255.0	254



المنطق فقط #

ولفهم كيف تم تحديد الفئات، نحتاج إلى فهم أن كل فئة من فئات IP هي

من فئة A

تماماً IANA باعتبار أنه الـ octet الأول من فئة A هو 00000000

التي تبدأ أول Bit فيه بالرقم 0. فكل ما بعد رقم 0 هو 00000000

وهو ما يقابله بالبتون الرقم 1. وآخر رقم قد يظهر بالبتون هو 127

منه هو رقم 01111111 الذي يقابل الرقم 127. لكنه تم حجز هذا الرقم للعالمية

أخيراً ما أصبح الـ Class A هو 1-126

فئة B

اعتبرت IANA أن أول Bit = 1 كما كان Bit = 0 من فئة A octet الأول

فكل ما بعد رقم 1 هو ما يقابله من البتون العشري 128

آخر رقم هو 10111111 وهو ما يقابله الرقم 191. فكل ما بين 128-191

فئة C

اعتبرت IANA أنه الـ Bit رقم 1 هو الـ Bit الثالث 0 فكل ما

أول رقم 11000000 وهو ما يقابله من البتون العشري 192

11011111 وهو ما يقابله من البتون العشري رقم 223. فكل ما بين 192-223

وبذلك تكونت هذه الأقسام Class

وضع لنا من قبل Class عدد الأجهزة "Host" في كل فئة Class 16 مليون

في A 16 ألف في B 16 ألف في C فنتعرف أنه ليس شبكة مكونة

من 16 جهازاً وإنما اختيرت Class نجد أنه يوجد عدد أجهزة ما بين 16 مليون

جهازاً فقط إرسال البيانات كبير جداً، فإما السويش أو الـ Hub ينقل

منه العنوان أنه هناك ما بين 16 مليون جهازاً رقم آخر حقيقة 16 فقط

كلية كبيرة اختيار Class غير مناسبة نظراً لعدد 16 مليون فيبدأ من

كل 16 مليون نقطة من البيانات وبالتالي 16 جهازاً لهم من سيكتلون لها

وعلينا ان نذكر ان الـ 16 مليون فقط هي التي يمكن ان تكون عناوين IP  
Loop من غير الشبكة وانما الشبكة تعتمد على الـ class غير المناسبة

مثال آخر: لدينا جهاز له شبكة بالطبع لا نستطيع ان نختار class  
صاحب الـ C class جهاز لأنه class أقل من عدد الأجهزة المراد تكميل شبكة  
في بالتالي نتقل إلى الـ class التالي ونجد ان الـ B class من عدد الأجهزة هو  
في class صاحب الـ 160 الف جهاز تقريبا نجد انه قابل لتكميل الشبكة صاحب  
الـ B class لكنه سيتم تحويل الـ 160 الف وليس الـ B جهاز وبالتالي  
تحت عملية اللوب وظيفتها الشبكة.  
وبحل هذه المشكلة نستخدم مايس ب الـ Subnetting

## Subnetting

باختصار الـ Subnetting هو عملية تقسيم للشبكة إلى شبكات أصغر  
فوائد كثيرة منها:

- ① تحسين أدار الشبكة
- ② تسهيل إدارة الشبكة
- ③ تحديد المشكلة بسهولة.

يجب وفهم عملية الـ Subnetting بصورة سليمة لأنه أنه نفهم عملية  
التحويل من عشري إلى ثنائي والعكس From Decimal To Binary  
وكذلك الـ From Binary To Decimal

## # التحويل بين العشري والثنائي #

وختاما نبقى انه الـ IP قد تكتب بالصورة العشرية مثلا  
أولها الصورة الثنائية التي لا تقدر على فهمه فقط وهذا الواحد والصفر مثل



10100111 - 00010001 - 00010001 - 00010001 - 00010001 - 00010001 - 00010001 - 00010001

مثالي عند من اتواحد من عدد 10100111 - 00010001 - 00010001 - 00010001 - 00010001 - 00010001 - 00010001 - 00010001

يتم التحويل بين الثنائي والعشري  
يتم التحويل بين الثنائي والعشري  
يتم التحويل بين الثنائي والعشري

1	2	4	8	16	32	64	128
---	---	---	---	----	----	----	-----

## ١١ التحويل من عشري إلى ثنائي

يتم التحويل من عشري إلى ثنائي عن طريق معرفة الرقم العشري للخرج عن ادمه  
نقوم بطرح الارقام السابقة من الرقم العشري فانه قبل الطرح دوره نتائج سلبية  
نضع تحت خانة الرقم 1 واذا لم يقبل الطرح نضع مكانه صفر والطرح بياض الرقم 10100111

مثال

كيفية تحويل الرقم 190 إلى رقم ثنائي

1	2	4	8	16	32	64	128
---	---	---	---	----	----	----	-----

نقوم بطرح الرقم 190 فنقوم بطرح 128 - 190 نجد ان تقبل الطرح والباقي هو  
62 - نضع 1 مقابل ال 128 أي مكانه ال Bit الأول من ال octet الأول  
بفرض انه 10190 ال octet الأول هو 10190 فكله الصورة 10190  
أو ونفسا 11 ف ال Bit الأول وبقية ال Bit ما زلنا لم نعرفها

نعود لمبدأ الطرح نجد الباقي على الطرح الأول هو 62 - نضع بطرحه  
ال 62 - 62 - نضع 1 مقابل الطرح فنضع واحد من ال Bit الثاني  
والباقي صفر ونقوم بطرح الباقي 30 - 62 - 30 - 30 - 30 - 30 - 30 - 30  
لا تقبل الطرح - نضع مكانه ال Bit صفر

1100 0000

فيكونه ليرقم الثنائي المقابل ل 190 هو

ما هي نتيجة تحويل الرقم 100 إلى رقم ثنائي

مثال آخر

100 76 32 16 8 4 2 1

نقوم بطرح الأرقام الثمانية

من الرقم 100 جاز قبل الطرح نضع واحد جاز قبل نضع صفر ونضيف

الطرح	100	76	32	16	8	4	2	1
الرقم	100	76	32	16	8	4	2	1
الطرح	100	76	32	16	8	4	2	1
الرقم	100	76	32	16	8	4	2	1
الطرح	100	76	32	16	8	4	2	1
الرقم	100	76	32	16	8	4	2	1
الطرح	100	76	32	16	8	4	2	1
الرقم	100	76	32	16	8	4	2	1

نلاحظ أنه بعد عملية الطرح نضع واحد إذا قبل الرقم ملبس الطرح ونزحل لمسيماً  
إذا اوجب ونطرح منه الرقم التالي . فمثلاً إذا لم يقبل الطرح نضع مكانه الصفر  
فيكون ناتج تحويل الرقم 100 من عشري إلى ثنائي

01111101

حول ال IP الثنائي إلى عشري  
192.168.1.50

مثال آخر

المثل

نقوم بطرح الرقم ثنائي ونطرح منه الأرقام الثمانية

octet 1	192	octet 2	168	octet 3	octet 4
1 = 100	192	1 = 100	168	0 = 100	0 = 100
1 = 76	76	0 = 76	40	0 = 76	0 = 76
0 = 32	0	1 = 32	40	0 = 32	1 = 32
0 = 16	0	0 = 16	8	0 = 16	1 = 16
0 = 8	0	1 = 8	8	0 = 8	0 = 8
0 = 4	0	0 = 4	0	0 = 4	0 = 4
0 = 2	0	0 = 2	0	0 = 2	1 = 2
0 = 1	0	0 = 1	0	1 = 1	0 = 1

11000000

10101000

00000001

00110010



1000000, 10101000, 00000001, 0010010

10A 71 PC 17 A 4 C 1

30

www.bbb.org

31

كلما في الصورة :

10A	75	40	17	—	—	—	—
-----	----	----	----	---	---	---	---

$$CE = 10A + 7B + 3C + 17 \therefore \text{Ans}$$

صالح حول الرقم الثاني 1111100 إلى رقم آخر

351

$$COC = 1CA + 7E + 5K + 17 + A + E = -$$

الرقم  $11111100$  الثامن = الرقم  $100$  العشري

مثال: تحويل IP العشري إلى الثنائي

	128	64	32	16	8	4	2	1	
octet <sub>1</sub>	1	1	0	0	0	0	0	0	= 192
octet <sub>2</sub>	1	0	1	0	1	0	0	0	= 178
octet <sub>3</sub>	0	0	0	0	0	0	0	1	= 1
octet <sub>4</sub>	0	0	1	1	0	0	1	0	= 50

نجمع من كل octet ما تحته واحد ونتجاهل الذي تحته صفر فيجاءنا الـ IP الثنائي: 11000000.10101000.00000001.00110100 = 192.178.1.50

وهكذا تعلمنا كيفية التحويل من عشري Decimal إلى ثنائي Binary والعكس  
كله ماخانة هذا التحويل ؟

الفاصلة من هذا التحويل أن البيانات تمر من الآلات لدى هيئة الرقم الـ Binary  
فلذلك رقم الـ IP فبغضاً أنه الجهاز A يرسل إلى الجهاز B عنوان الـ IP  
عند الجهاز المرسل يقول الـ Binary ويرفها الآلات - إلى أنه يصل إلى الجهاز  
المستقبل ويقوم بترت النتيجة من الجهاز B بتحويل الرقم من Binary إلى Decimal  
وقدنا تتم عملية نقل البيانات .

ملاحظة هامة: عند تحويل الأرقام من عشري إلى ثنائي والعكس هناك أرقام سهلة  
تحويلها لتسهيل المائل علينا وها هم الجدول

0	128	192	224	240	248	252	254	255
00000000	10000000	11000000	11100000	11110000	11111000	11111100	11111110	11111111



# # Subnetting #

① تحديد عدد ال Host وال Subnetmask المناسب (٥)

تقسيم شبكة 194.1.1.0 / 24 إلى 3 شبكات

3 classes

Class A (1 : 126) → 255.0.0.0  
 Class B (128 : 191) → 255.255.0.0  
 Class C (192 : 223) → 255.255.255.0

نقد بفرعنا ان عدد أجهزة الشركة هو ٥٠ جهاز فربما أنه غير مناسب  
 واحدة نجد أن في Class لا يناسب عدد أجهزة قليلة وازدادت Class B  
 مبالغ من ارقام عدد أجهزة الشركة بالنسبة لعدد الأجهزة لدى هذا العمل  
 في هذه الحالة نقوم بتقسيم Subnetmask مناسب ذلك العدد الأجهزة  
 اعتباراً Subnetmask = 255.255.255.0 ولكن نقوم بتقسيم Subnetmask مناسب لعدد الأجهزة  
 نتقدم القانون التالي

$$\text{hosts} = 2^h - 2$$

وال Host هو عدد الأجهزة

نظراً لعدد أجهزة هو ٥٠ من القانون  $0 = 2^h - 2$

نجد أن أقرب أسس يناسبه تقريبا هو ٥٠ حيث يكون الأس هو ٩

$$510 = 2^9 - 2$$

أي عدد الأجهزة التي استطيع وضعها في نفس ال Subnetmask هو ٥١٠  
 الآن سنتقسيم صنف ال Subnetmask المناسب عنه طريق اعتبار ال h الأس  
 عبارة عن اختيار منضوع ٩ وهذا الأس هو ٢٥٥.٢٥٥.٢٥٥.٠  
 اختيار من القيمة وما بعدها يكون واحد - ٢٥٥.٢٥٥.٢٥٥.٠

Subnetmask ٢٥٥.٢٥٥.٢٥٥.٠

$$255.255.255.0$$

هو ←

الخلاصة في عدد الاضمار من ال Subnetmask حدد عدد الأجهزة في هذه الشبكة على طريق

$$\text{host} = 2^h - 2 \quad \text{عدد الاضمار} \quad 9 \quad 2^9 - 2 = 512 - 2 = 510$$

مثال آخر مثال آخر ماهو ال Subnet mask المناسب لشركة - 5000 جهاز ؟

$$5000 = \text{Hosts}$$

$$5000 = 2^h - 2 \quad \text{حيث } h \text{ هو عدد البتات في ال Subnet mask}$$

بعد طريقة الانتهاء اننا الى سب نجد ان  $h = 13$  حيث ان سب عدد قسمة لـ 5000 هو  $2^3$  حيث انه  $2^{12} = 4096$  وهذا غير مناسب .

$h = 13$   $\therefore 2^{13} - 2 = 8190$  - هو الذي استطيع وضعهم في شبكة واحدة .  
فيكون لدى 13 حيز لضعهم منه اليهيد وما بعدهم تضعهم وما به

11111111.11111111.11100000.00000000

ونقول الرقم التالي " Binary " الى رقم عشري " Decimal "

فيكون Subnetmask 255.255.224.0 وهو ال

المناسب لعدد أجهزة 5000 حيث انه يسع بـ 8190 جهاز في شبكة .

\* تكلمنا في المقالة السابقة عن تحديد ال Subnetmask ولم نتكلم عن ال IP  
والآن نتكلم عنه حيث في مثال ال - 5000 جهاز لدينا ال Subnetmask وهو عنوان  
مهم ولكن لم نتكلم عن عنوان ال IP كيف يتم تحديده لـ 5000 جهاز وهل كل  
البيانات متاحة أم هل هناك ما لا - نطيع استنتاجه ؟

كل نقوم بإيجاد وتحديد عنوان لكل جهاز ولذلك معرفة المتاح لـ 5000 عند عنوانه  
أجهزة الشركة نختار ابتداءً IP عنوان من ضمن ال البيانات التي  
أوردناها للأجهزة . مثال نختار ال IP 100.100.100.10 لـ  
أختار هذا ال IP فعدد عناوين ال التالي

Subnet	First valid IP	Last valid IP	<del>Subnet mask</del> Broadcast ip



1) إذا كانت الأرقام العشرية هي الـ Subnetmask فحينئذٍ نكتب Network address

في عنوان الـ IP الذي يأتينا به في أيدينا الشبكة ولكن يتم

تحديد الـ Subnetmask لهذا نقوم بتحويل الـ IP العشري إلى

ثنائي نجد أنه الـ IP بالصيغة الـ Binary هو

01100100 . 01100100 . 01100100 . 00001010

ثم نقوم بتحديد على الـ Subnetmask المناسب له 255 جهاز كما في المثال الذي

عددناه ونضع بالتيار (1+1) (1+1) (1+1) = 255

11111111 . 11111111 . 11100000 . 00000000

01100100 . 01100100 . 01100100 . 00001010

01100100 . 01100100 . 01100000 . 00000000

100 . 100 . 96 . 0

ثم نحول الناتج إلى عشري فيكون

:- عنوان هذه الشبكة Network address أو ما يسمى Subnet هو

2) تحديد الـ Broadcast IP

آخر خانة من الـ Broadcast IP وهو العنوان الذي به طريقة من نتيج إرسال

البيانات لكل الشبكة وهو آخر IP في الشبكة ولتقديم الحماية لأحد الأجهزة مثله

مثل الـ Subnetmask حيث هو عبارة عن Network address وهو (2-1) من القانون  $2^x - 1$  hosts

طريقة تحديده هي عن طريق الـ Subnetmask نضع ونضع تحته الـ IP العشري

بالصيغة الـ Binary

Subnetmask 11111111 . 11111111 . 11100000 . 00000000

العنوان IP 01100100 . 01100100 . 01100100 . 00001010

وبناءً على العنوان في الـ Subnetmask نضع كما باللون الأحمر ما كانت الواحدة من الـ IP العشري

ينزل كما هو وما تحت الأجهزة ينزل وما به بالتالي تكون النتيجة

ما تحت الأجهزة أصبح واحد

01100100 . 01100100 . 01111111 . 11111111

نقوم الآن بتحويل الـ Binary إلى Decimal فيكون 100.100.127.255

لنكتشف ما بعد الـ Subnet mask : (Broadcast)  
 هي الأخيرة من الحايطات الافتراضية لها هي 255.255.255.255  
 بعد 10.10.10.10 هو آخر IP  
 لذلك الأخيرة المركزية للجدول هي :

Subnet	First valid IP	Last valid IP	Broadcast
100.100.95.0	100.100.95.1	100.100.127.255	100.100.127.255

بعد تحديد المتاح من الأجهزة نستطيع الآن معرفة أجهزة الشبكة وانظر  
 IP لكل جهاز فلماذا ذكرنا الـ Subnet mask الذي هو 255.255.255.255 نستطيع  
 أنه يجمع 8190 جهاز في هذه الشبكة .

### ٥ تحديد عدد الشبكات من الـ Subnet mask

بفرض في المثال السابق أنه الشركة صاحبه الـ 8190 جهاز أرادت زيادة  
 أجهزة الشركة بعد 8190 جهاز آخر أو حتى 8190 جهاز نلاحظ  
 أن الـ Subnet mask يجمع 8190 جهاز في الشبكة فبعض هذه زيادة عدد الأجهزة  
~~مطلوبه~~ هو أن يكون محكوم بعد 8190 في الشبكة فالحل الطريقة التي نستطيع زيادة  
 عدد أجهزة الشركة ؟

بالطبع لا نستطيع أنه نبدأ المثال من جديد باعتبار أننا جهاز ونحسب الـ Subnet mask  
 والـ Hosts والـ Valid IP فقلنا أنه أجهزة الشركة هو 8190 أو بروتينات  
 أو سيرفر الشركة أصبح الـ IP وبالتالي يجب جداً تغييرها فالحل من ذلك  
 قلنا أنه الـ Subnet mask تقسم على أكثر من شبكة وكل شبكة على  
 8190 جهاز حسب المثال السابق قلنا كيف يتم تحديد جهاز ؟

نلاحظ أن الـ Subnet mask هو 11111111.11111111.11111111.11111111

لنستطيع معرفة عدد الشبكات الـ Subnet mask عبر طريقة معرفة عدد العناوين من



في Octet الذي يحتوي على 8 بتات، ما عدد البتات التي يمكن استخدامها في الـ Subnet  
 100.100.100.00000000

في الـ Octet رقم 3 هو الذي يحتوي على 8 بتات، ما عدد البتات التي يمكن استخدامها في الـ Subnet  
 100.100.100.00000000

$$\text{number of Subnet} = 2^n$$

←

عند  $\text{number of Subnet}$  عدد البتات في الـ mask و (n) هي عدد البتات  
 في الـ Octet الذي يحتوي على 8 بتات، ما عدد البتات التي يمكن استخدامها في الـ Subnet

$$n = 8 - \text{mask}$$

ولكن عدد البتات في شبكة لا يتغير Blocksize ولا يتغير عدد البتات

ما قبل آخر واحد من الـ Subnet mask هو الأرقام الأساسية (1 2 4 8 16 32 64 128 256)  
 نتجبه أن آخر واحد يقابل (256) فنزيد من الـ Octet الثالث مكانه الـ Blocksize  
 نزيد 256 من كل عنوان شبكة فيصبح الجدول

Subnet	First Valid IP	Last Valid IP	Broadcast
100.100.96.0	100.100.96.1	100.100.127.255	100.100.127.255
100.100.128.0	100.100.128.1	100.100.159.255	100.100.159.255
100.100.160.0	100.100.160.1	100.100.191.255	100.100.191.255

و متعلق ليس 8 شبكات من الـ Subnet mask (mask) لكنه كل شبكة  
 ليست في الأخرى إلا في غير الـ Subnet mask  
 كل شبكة تحتوي على 190 جهاز

هذا

انصح في كل المتعلقة الشبكات ان تستطيع فهم عمل الأجهزة من  
طريقة عمل النظام من الـ Subnet mask من فهم ان تستطيع فهم الشبكات  
من الـ Subnet mask عن طريق عمل الواجب

عمل الأجهزة =  $C - N$  حيث  $N$  هو عدد الأجهزة  
عدد الشبكات =  $C$  حيث  $N$  هو "Network" هو عدد الواجبات في الـ Host الذي يكون  
وأيضا أصغر أو أنه يكون آخر 01 من الـ Subnet mask

# الخلاصة الـ Subnet mask يفسر جزئية جزئية الشبكات Network  
وهي الشبكات ذات القيمة 1 هي جزئية على الأجهزة الـ Hosts وهي الشبكات ذات  
القيمة 0

class C	Network Bits	Hosts Bits
	11111111.11111111.11111111	00000000

# شراء IP

يستطيع الناس ان يطور أجهزة الشبكة الخاصة به بتأويل IP وهو انه  
يقوم بدفع أو مبلغ من المال لكنه من هذه الحالة لم يستطيع الاتصال بشبكة الانترنت  
هذا النوع هو الـ Private IP وهو داخل الشبكة ولا يستطيع من طرفه استخدام  
الدخول على الانترنت

# الـ Public IP هو نوع آخر من IP يقوم صاحبه الشبكة بشرائه من  
مزود الخدمة مثل شركة المصرية للاتصالات عن طريقه هذا الـ IP تستطيع  
الدخول على الانترنت

بالطبع قد لا يختلف عنوان الـ Private مع آخر الـ Public لكنه الأصغر الذي تقدمه  
لشركة المزودة للخدمة هو الذي يسمي للدخول للانترنت



## # مصطلح ال CIDR

ال CIDR هو المصطلح المستخدم في Subnetting وهو اختصار لـ Classless Inter-domain Routing و "Supernetting".

ملاحظة: هو البلوك الذي حصل عليه رأياً من تقسيم الشبكات بناءً عليه سواء  
معطى عدد الأجهزة أو عدد الشبكات.

مثال ال CIDR  $\rightarrow$  مثال  $\leftarrow 205.5.5.0/24$

الجزء الأول من هذا ال CIDR  $[205.5.5.0]$  هو عبارة عن ال Subnet  
أو يعني آخر هو عنوان الشبكة ال Network ID و أما الجزء الثاني من ال CIDR  
وهو الرقم  $[24]$  كما في المثال فإنه عبارة عن ال Subnetmask وهو يعني أنه يمثل  
عدد البتات ذات القيمة 1 في ال Subnetmask

مثال آخر

Subnetmask  $\rightarrow 176.7.0.0/16$  Network address

## # تجاربه على ال Subnetting

مثال 1: لدينا ال CIDR  $\leftarrow 205.5.5.0/24$  والطلب منك تقسيمه

إلى 3 شبكات وتحديد ال Network address و Broadcast و Valid Ips لكل شبكة ؟

الحل

أولاً عن طريق ال Subnetmask فما ال CIDR ال IP من الكلاس C

عدد الشبكات  $= 2^N$  :  $2^3 = 8$  :  $2^N = 8$  :  $N = 3$

نتردد عدد العوايد فما ال ال أصغر قيمة 3 وعنايد

11111111 . 11111111 . 11111111 . 11100000

ف نقوم بالقول من مثال آخر  $\leftarrow 255.255.255.224$

ف تكون أول شبكة من ال 3 شبكات ال CIDR الأولى  $\rightarrow$  Networks

$\leftarrow 205.5.5.0/27$  ال ال الجديدة

محدد للشبكة سايبر أوميدون "step" وهو قيمة أخرى ضمن الـ octet المحدد في الشبكة السابقة

~~205.5.5.1~~

~~205.5.5.31~~

شبكة الـ step = 32

205.5.5.0/27

الـ شبكة الأولى هي

205.5.5.1

هو First valid IP

205.5.5.30

هو Last valid IP

205.5.5.31

هو Broadcast

وعبرتنا الـ Broadcast للشبكة الأولى عبر طريقة زيادة الـ step وهو 32

لنا شبكة الأولى من الـ octet الأخير فتكون الشبكة الثانية

هي 205.5.32 ونطرح 32 من الـ Broadcast Broadcast الشبكة السابقة

network address

valid

Broadcast

الشبكة الثانية 205.5.32/27

(5.62 : 5.93) 5.63

الشبكة الثالثة 205.5.64/27

(5.94 : 5.125) 5.95

الشبكة الرابعة 205.5.96/27

(5.126 : 5.157) 5.127

الخامسة 205.5.128/27

(5.158 : 5.189) 5.160

السادسة 205.5.160/27

(5.190 : 5.221) 5.192

السابعة 205.5.192/27

(5.222 : 5.253) 5.223

مثال مطلوب 3 شبكة مع العلم انه الـ CIDR هو 167.7.0.0/6

مثال

الكل

عدد الشبكات المطلوبة = 3

3 = 2^N = 9

حيث شبكة له 9 جهاز وهو أقرب من قيمة الحصول عليه

مقارب لـ 3 جهاز

نقوم انكس بإضافة 9 وصاية للماسك للحصول على الماسك الجديد

11111111.11111111.11111111.00000000

الماسك الجديد هو 25 في الشبكات الجديدة 167.7.0.0/25



نقوم الآن بملأها من 128 إلى 255 Step عند ترتيبها  
 ما يلاحظ أن قواعد الشبكة العنصرية الخاصة بالترتيب هي 128  
 - ترتيب 128 هو 128 الأخير هي 128 فكل واحد منها يصل إلى الشبكة  
 الأخيرة

الشبكة الأولى 167.7.0.0/25  
 الشبكة الثانية 167.7.0.128/25  
 167.7.1.0/25  
 167.7.1.128/25  
 167.7.2.0/25

وقدنا إلى أنه نصل إلى شبكة

مثال 3 مطلوب شبكة مع العلم أنه ال CIDR هو 12.0.0.0/8

الحل

عدد الشبكات =  $2^N$  :  $C = C_{\text{new}}$

$N = 8$  هي الناتج هو 256 أمربا شبكات 200 حصة  
 أو أنه ترتيب 8 وهي من المسألة الجديدة

00000000.00000000.00000000.00000000

في المسألة الجديدة هو 16 والشبكة الأولى هي 12.0.0.0/16

الآن نقوم بملأها ال Step وهو آخرها من المسألة ونجد ما يغالبه هو

① ترتيب ال Octet الثاني هي هو مكان آخر واحد بقدر ①

في الشبكات هي

الشبكة الأولى 12.0.0.0/16

الشبكة الثانية 12.1.0.0/16

الشبكة الثالثة 12.2.0.0/16

الشبكة الرابعة 12.3.0.0/16

وقدنا إلى أنه نصل إلى شبكة

مثال ٤

لدينا في الشبكة 210.10.10.0/24 تم تقسيمها إلى شبكات  
بحيث يكون لكل شبكة 64 جهاز

الحل

هذه المسألة المطلوب فيها ليس عدد شبكات لكنه أنه يُطلب من كل شبكة

٦٤ جهاز في نفس حجم القانون  $Hosts = 2^h - 2$

عدد الأجهزة =  $2^h - 2$

$64 = 2^h - 2$

فإذا  $h = 7$  فيكون الناتج  $2^7 - 2 = 128 - 2 = 126$  جهاز

$64 = 2^h - 2$   $66 = 2^h - 2$   $68 = 2^h - 2$   $70 = 2^h - 2$   $72 = 2^h - 2$   $74 = 2^h - 2$   $76 = 2^h - 2$   $78 = 2^h - 2$   $80 = 2^h - 2$   $82 = 2^h - 2$   $84 = 2^h - 2$   $86 = 2^h - 2$   $88 = 2^h - 2$   $90 = 2^h - 2$   $92 = 2^h - 2$   $94 = 2^h - 2$   $96 = 2^h - 2$   $98 = 2^h - 2$   $100 = 2^h - 2$   $102 = 2^h - 2$   $104 = 2^h - 2$   $106 = 2^h - 2$   $108 = 2^h - 2$   $110 = 2^h - 2$   $112 = 2^h - 2$   $114 = 2^h - 2$   $116 = 2^h - 2$   $118 = 2^h - 2$   $120 = 2^h - 2$   $122 = 2^h - 2$   $124 = 2^h - 2$   $126 = 2^h - 2$

ما نريد تقسيمها إليه هو 64 ~~جهاز~~ جهاز في كل شبكة.

\* لكن نقوم بتقسيم الماسك الجديد نضع  $h$  عبارة عن أصغر، أما أننا  
نضع ٦ أصغر، هذا الباقي هو

11111111.11111111.11111111.11111111

255.255.255.192

وهو

الماسك الجديد زاد فيه عدد الوطايه بمقدار ٤، فيكون  
الشبكات هي

الشبكة الأولى

210.10.10.0/26

210.10.10.64/26

210.10.10.128/26

210.10.10.192/26

في شبكة سيكون في ٦٤ جهاز والمحتاج ٤ شبكات فقط هي

عدد الوطايه في الـ octet الأخير صاحب أرقامه هو

عدد الشبكات =  $2^4 = 16$  شبكات



مثال ٥ مطلوب حساب جهاز فورييه شبكة مع العلم أنه الشبكات هو 172.16.0.0/16

بداية

$$C - hC = \text{عدد الشبكات}$$

$$C - hC = 0$$

$$C - 9C = 0$$

$$0.0 = C - 01C = 0$$

عليه أنه وضع 0.0 جهاز في الشبكة الواحدة

نقوم الآن بوضع 9 أصغار في الـ mask الجديد

11111111.11111111.11111111.00000000

هناك 23 الشبكة

نحدد الآن الـ step وهو قيمة ما يقابل آخر واحد نجد أنه 8

ننجز به قيمة الـ det الثالث بقدر

الشبكات هذا

172.16.0.0/23 الشبكة الأولى

172.16.2.0/23

172.16.4.0/23

172.16.6.0/23

حتى يصبح لدينا عدد من الشبكات ننتج حساب به طريقة  $C^h$  حيث  $h$  هو عدد الوايت في الـ det الثالث  $C^h = 128$  شبكة

مثال 6

إذا كان الـ cidr هو 10.0.0.0/8 مطلوب تقسيمه إلى شبكات بحيث

تكون مساوية لجهاز فورييه شبكة

الكل

$$C - hC = \text{عدد الشبكات} \quad C - hC = 1 \text{ مساوية}$$

$$C - hC = 1 \text{ مساوية} \quad 10 = h \quad C - 10C = 10.0.0.0 \text{ جهاز في الشبكة}$$

نقول الآن الـ  $h$  إلى الأصغار في الـ mask الجديد

11111111.11111111.11111111.00000000

حفظنا الخانات لثلاثة بوابات (3)

تقوم بوابات حاسب ال Step 3 بحساب  $2^x$   
في الخانات هي

الأول	10.0.0.0/22
الثاني	10.0.4.0/22
الثالث	10.0.8.0/22
الرابع	10.0.12.0/22

ويكون لدينا 4 شبكات ~~في~~ يمكن حسابها بطريقة  
عدد الشبكات =  $2^x$  حيث  $x$  هو عدد الزيادة في البتات الوطانية  
الناشئة الأولى أو عشرين آخر العنصرية الزيادة في الخانات الجديدة.  
عدد الشبكات =  $2^4$

عدد الشبكات = 16, 32, 64 شبكة

VLSM

ال VLSM هي اختصار لـ Variable length Subnetting وهي عملية يتم من خلالها تقسيم  
الشبكة الرئيسية "Cidr" إلى عدد من الشبكات الفرعية غير المتساوية  
بحسب عدد ال Hosts بخلاف ال Subnetting الذي يكون فيه عدد ال Hosts متساوي  
في كل شبكة نريد هنا ويتم ذلك بطريقة جعل ال Subnetmask متغير من كل شبكة  
طريقة

مثال

إذا كان ال Cidr هو 192.168.10.0/24 نريد تقسيم هذا ال Cidr  
إلى 5 شبكات الأول ربع ما جهازه 50 والثاني 50 والثالث 20  
والرابع 10 والخامس 5 لكن منطوق 5 أجهزة فما هو الطريقة ؟

الحل

نقوم بتقسيم هذا ال Cidr إلى أكثر من Subnetmask ويتم ذلك



لنذكر كل فئة من هذه الشبكات

١- الشبكة الأولى: ٢ جهاز

$$\text{عدد الشبكات} = 2^0 = 1 \quad \text{عدد العناوين} = 2^8 = 256$$

$$\text{من } 256 - 2 = 254 \quad \text{من } 256 - 2 = 254$$

٢- الشبكة الثانية: ١٥

تقع ١٥ عناوين لعنوان الماسك الجديد

$$10000000 - 11111111 - 11111111 - 11111111$$

٣- الماسك الجديد هو 25

$$192.168.10.0/25 \quad \text{في الشبكة الأولى هو}$$

والـ stop هو 1٢٨ متبقية ما قبل آخر وانه

٤- الشبكة الثانية هي متوازنة هو 192.168.10.128

٥- الشبكة الثانية: ٥ جهاز

$$\text{عدد الشبكات} = 2^0 = 1 \quad \text{عدد العناوين} = 2^8 = 256$$

عدد الأجهزة في الشبكة ٦٤

تقع ٦٤ عناوين لعنوان الماسك الجديد

$$10000000 - 11111111 - 11111111 - 11111111$$

٦- الماسك لهذه الشبكة هو [26]

$$192.168.10.128/26 \quad \text{في الشبكة هو}$$

فقد الـ stop نجد أنه [٦٤]

٧- الشبكة الثالثة هو 192.168.10.192

٨- الشبكة الثالثة: ٣ جهاز

$$2^0 = 1 \quad 2^1 = 2 \quad 2^2 = 4 \quad 2^3 = 8 \quad 2^4 = 16 \quad 2^5 = 32 \quad 2^6 = 64 \quad 2^7 = 128 \quad 2^8 = 256$$

تقع ٥ عناوين لعنوان الماسك الجديد

$$10000000 - 11111111 - 11111111 - 11111111$$

في الشبكة هو (27)

في الشبكة هو 192.168.10.192/27

نجد ان Step نجد انه (28)

في الشبكة هو 192.168.10.224

الشبكة الرابعة هـ أجهزة عناوين 192.168.10.224

$$0 = c - 8 = c - 8 = 0 \quad 0 = c - 8 = 0$$

منه الأجهزة 7 في الشبكة

تقع رأس 13 أصغار للـ 13 الجديدة

11111111 . 11111111 . 11111111 . 11111111

في الشبكة الجديدة هو 29 في الشبكة هو 192.168.10.224/29

نجد ان Step نجد انه (28)

في الشبكة هو 192.168.10.232

الشبكة الخامسة

$$0 = c - 8 = c - 8 = 0 \quad 0 = c - 8 = 0$$

الـ 13 لهذه الشبكة هو (29)

في الشبكة هو 192.168.10.132/29

في اجمالي الشبكات

- 1 192.168.10.0/25
- 2 192.168.10.128/26
- 3 192.168.10.192/27
- 4 192.168.10.224/29
- 5 192.168.10.232/29



مثال: إذا كان لدينا شبكة 223.10.10.0/24 والمطلوب هو تقسيمها إلى  
 5 شبكات الفرعية مع الحفاظ على أكبر وأصغر وعناوين من الشبكة  
 الواصلة بين الشبكات ونود في 29 عقدة ما هو الحل؟

أو شبكة هو 223.10.10.0/24

(1) شبكة الأولى 0 جهاز

$$hosts = 2^h - 2$$

$$50 = 2^6 - 2$$

$$50 = 64 - 2$$

$$hosts = 62$$

أحمد السويح به 60 جهاز من هذه الشبكة ؟ نقوم الآن بزيادة أحدهم إلى 7 أصناف  
 وبإبقاء وتنايه للوصول إلى العاشرة الجديدة .

$$Newmask = 11111111.11111111.11111111.11000000$$

في الشبكة الأولى تتناوب 223.10.10.0/26

بحسب الآلة ال Step فبأنه = 64 = 2<sup>6</sup> = 64 أو ما يكافئ آخر ما ص

في بداية الشبكة الثانية هي 223.10.10.64

(2) الشبكة الثانية بدأت هي 223.10.10.64 ومطلوب 10 أجهزة

$$hosts = 2^h - 2 \quad 10 = 2^4 - 2$$

أحمد السويح به 10 جهاز ؟ نضع الآلة 2 أصناف وبإبقاء وتنايه .

$$Newmask = 11111111.11111111.11111111.11110000$$

في الشبكة هي 223.10.10.69/28

نقوم بحساب ال Step = 2<sup>4</sup> = 16 = 2<sup>4</sup>

في الشبكة الثالثة هي 223.10.10.80

(3) الشبكة الثالثة بدأت هي 223.10.10.80 وبها أجهزة (2)

$$hosts = 2^h - 2 \quad 2 = 2^2 - 2 \quad 2 = 2^1 - 2$$

$$Newmask = 11111111.11111111.11111111.11111100$$

المنطقة الأولى من 223.10.10.80/30  
 المنطقة الثانية من 223.10.10.80/30 Step 2

	Network ID	First valid Ip	Last valid Ip	Broadcast
المنطقة الأولى	223.10.10.0/26	223.10.10.1	223.10.10.62	223.10.10.63
المنطقة الثانية	223.10.10.64/28	223.10.10.65	223.10.10.78	223.10.10.79
المنطقة الثالثة	223.10.10.80/30	223.10.10.81	223.10.10.82	223.10.10.83

## # Class D & E #

لأغراضنا منقسمت الـ IANA قاست بتقسيم الأيبيجات إلى classes ذكرنا  
 من A B C & D

+ لكن هناك Class D وهو ( 224 - 239 ) أي أنه أي Ip يبدأ  
 الـ octet الأول منه برقم من 224 إلى 239 فهو Class D وهو خاص  
 بالـ multiCast ← ليس مقرر على CCNA والـ multiCast  
 يختلف عن الـ Broadcast حيث أنه لا يُرسل الرسالة لكل أجهزة  
 الشبكة بل يرسل الرسالة لجزء معين من الشبكة.

\* Class E ← ( 240 : 255 ) هذا الـ Class أنت لا تستخدم  
 المستقبل لكن نتيجة التوسع في استخدام الأيبيجات ظهر حيل جديدة  
 من الأيبيجات هو IPv6

## The Ip 127.0.0.1 #

لأغراضنا Class A ( 1 : 126 ) و Class B ( 128 : 191 )  
 نأخذ الـ Ip الذي رقمه 127  
 يستخدم هذا الـ Ip ( 127 ) في علمه Loop Back



[illegible]

## # Subnetting 11.0.0.0/24 #

قد يعطى من الاختبار مصنوعة من الايوانات في سكة واحدة و يطلب من انه انه  
أدب Subnetmask لهذه الايوانات .

مثال: لنلاحظ المبروك من الرياضات

$$10.0.0.5 \quad \{ 10.0.20.200 \quad \{ 10.0.180.5 \quad \{ 10.0.200.200$$

Subnetmask 255.255.255.0

351

① معرفة ال Subnetmask المناسب لهم لتحديد أصغر IP وأكبر IP على الشبكة معرفة

رقم الـ octet غير القابلية للتقسيم  $I_p$  فاجد أنه الجزء 10.0 قابلية - غير

٥. ٥. ٥. ٥. ٥ IP هو

عائزہ 200:200:200-10

٥) نقوم بتحويل الـ octet الذي حددنا على أنه أصغر Ip إلى Binary

Ipjoi  $\rightarrow 0 = 00000000$

اگر  $200 = 11001000$  ہے

② ننظر البيت رقم ١ اذا كان فيه كتابه سوار صفر مع صفر او واحد مع واحد

يُنْقَلُ الرُّقْمُ ١ صَلَاحُ كُلِّ لَدِيَّةٍ الثَّالِثُ نَوَاشِيهِ يُنْقَلُ مَا وَجَدَ مِنْ هَؤُلَاءِ لَكُمْ إِذَا الْخُطْبَةُ

البيت سوار من مع واحد أو واحد مع من ينزل ~~هو~~ كل ما بعده أصفا

00000000

11001000

00000000 - اختلاف البت الأول سلكي 1 بت سلكي الثاني أحادي

Subnetmask المناسبة هي

255.255.0.0

مثال آخر  
لديك المجموعة التالية من الـ IP addresses ما هو الـ Subnetmask المناسب؟

10.0.2.200 & 10.0.10.5 & 10.0.5.200 & 10.0.7.5

الحل

① قم بأصغر ما أكبر IP

الأصغر هو

10.0.2.200

الأكبر هو

10.0.10.5

② نقوم بتقسيم الـ octet الأول بعد الثوابت نجد أنه الـ octet الثالث ونقوم بتحويله إلى Binary

الـ 2 = 00000010

الـ 10 = 00001010

③ ما كانه متساويين واحد ولو اختلفنا سلكي وما بعد أحادي

11110000

الناجح هو

Subnetmask المناسبة هي

255.255.240.0


الـ 255.255  
يترك الجزء المشترك من جميع الـ IP addresses وهو 10.0



صالحه بنت عبد الله

$$V(\mathbb{R}) = V(\mathbb{C}) = V(\mathbb{A}) = \emptyset$$

الحمد لله رب العالمين، من أجل اختيار عنوان هذا الكتاب  
عن: *Dr. Mohamed Elmaghrabi* الأستاذ المساعد في جامعة القاهرة



Binary : 10101010 Subnetmask : 255.255.255.0

uuuu . vvvvv - wwww - yy Cccc

نقوم الآن بتقديم الـ  $step$  وهو  $h$  في  $h$  من الأضلاع  
مقلية بتدويرها أيضاً عن طريقه من  $h$  إلى  $c$  واعد من مضاعفات الـ  $c$   
في  $step = c = 0$  : نضيف  $c$  في الـ  $octet$  الأخير  
في الـ  $NetworkIO$  التالي فهو

192.115.103.96/27

# قاتل انكسار و تصغير حجم الـ IP Subnetting و VLSM

# القوايض المستخدمة في هذا الباب #

① Number of hosts  $= 2^h - 2$

حيه كذا في الاصل

② number of networks =  $2^N$

حيث لا يوجد عند الوفاة الزائدة على الحد الأقصى

③ BlockSize "step" =  $2^h$

صحة هـ عند الاضطرار نزل الـ  $\det$  النسبة الضعيفة وحيث اننا نرى ان النسبة الضعيفة هي النسبة التي نزل عنها النسبة القوية

# The Router

أما كونه جهازاً خاصاً فهو من الراوترز - يتكلموا وإخادها تلمع مع نظام تشغيل  
وتنفيذ البرامج الراوتر أصبح الكلام الذي على أساسه يتكلم الراوتر  
يتكلم الراوتر من

① معالج CPU

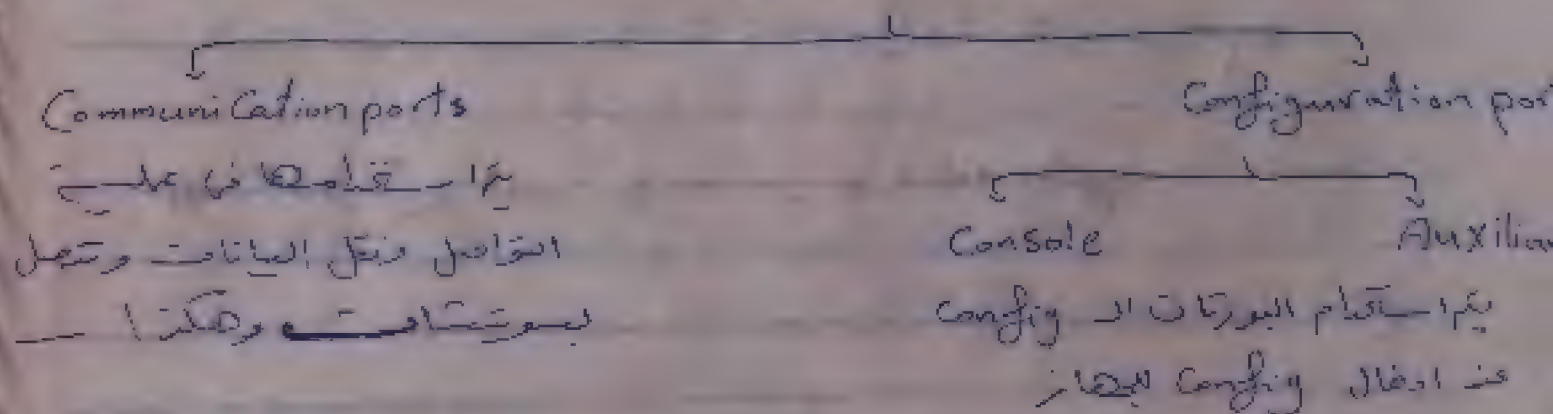
② RAM - يتم تخزين البيانات عليها لتتم نقلها إلى الذاكرة الغير متطايرة

③ Flash memory - يتم حفظ الـ IOS Image

④ NV Ram - يتم حفظ الـ Config عليها ولا تفقد بانقطاع التيار

⑤ Rom - معلومات عامة عن الراوتر

## بورتات الراوتر



• تلمع إضافة مودم من الاحتياج سواء مودم ethernet أو سيريال

• Serial port - هذه البورتات تتميز بأنها تستطيع التحكم في السرعة حيث  
أن ethernet تلمع التحكم في تقليل السرعة 10 ميجا أو 100 ميجا  
تلمع السيريال تتحكم في 3000 - 500000 و هكذا  
وأيضا فتتم السيريال تربط بين الشبكات الواسعة الـ WAN  
وأيضا يتم توزيع سرعة من الراوتر إلى الراوتر آخر وتسمى تقنية Back to Back



Host  
(DTE)  
Data Terminal equipment

Router  
(DCE)  
Data Communication equipment

هذه هي المسميات التي نستخدمها في (V.35)

- يتم توصيل الطرف A من Router بجهاز الكمبيوتر (Host)
- يتم توصيل الطرف B من Router بجهاز Data Communication equipment

## Router Configuration

تتضمن إعدادات الراوتر مع أوامر التكوين (Configuration) وهي:

- ① الدخول للجهاز
  - ② الدخول لـ Privileged
  - ③ الدخول لـ Global Configuration
  - ④ تفعيل الـ Telnet-SSH وورد واجهة الـ Console
  - ⑤ تغيير اسم الجهاز و إعدادات الباس
  - ⑥ تمكين البورت وأوامر الـ Help
  - ⑦ أوامر الـ Save و Show
- لمراجعة هذه الـ Config فراجعها من باب المراجعة.

## # تحديد الـ Gateway

ابتداءً إذا كان لدينا شبكة فـأستطيع أن أعمل الـ Communication بين هذه الشبكات مع طريقة الراوتر فكل بورت IP من الشبكة المتصلة به هذا الـ IP هو الـ Gateway لهذه الشبكة.

مثال: الموزع F0/0 في حقله IP 192.168.10.1 شبكة 192.168.10.0/24

```
Router > en
Router # Config T
Router(Config) # int F0/0
Router(Config-if) # No shutdown
Router(Config-if) # ip address 192.168.10.1 255.255.255.0
```

• وغالباً نلاحظ ان بعد اتمتة آخر IP في الشبكة أمارات IP وهذا ليست هي  
 عند تدقيقهم فاصالة ان سيان  
 • لنضع كتابه ان على interface في خرج الامر Show IP interface Brief

## # Vlan gateway

الطريقة السابقة كانت الطريقة فاصالة الشبكة العادية فكل شبكة تابعة  
 لـ واحد بعدد من الشبكة ونعطيها البورت الفاصل عليه هذه الشبكة. لكن في حالة  
 الـ Vlan يختلف الامر حيث تقع الـ Vlan بتقسيم الشبكات  
 الى شبكات وصية وبالتالي كل Vlan يحتاج الى gateway فبعضه انه كل  
 الـ Vlan تكون متصلة على بورت واحد فها هو الحل.

### ① الطريقة باستخدام الراوتر

- ① جعل البورت من الصورتين الذي يتصل بالراوتر Trunk
- ② بالنسبة لبورت الراوتر جعله up به طريق أمر No shutdown
- ③ تقسم البورت الى Subinterface ونعطي كل (Subint) IP من الـ Vlan

مثال: لدينا شبكتين Vlan10 والاولى Vlan20 والباقي Vlan30 وهذه متصلة  
 على البورت F0/0 في الراوتر ونريد ان نغنيها بعدد واحد فها هو الحل.



① في التكوين التالي، كيف يتم تكوين الـ Subinterface على الـ Router؟  
 Router(Config-if) # ~~subinterface~~ ~~mode~~ ~~Trunk~~

② في التكوين التالي، كيف يتم تكوين الـ Subinterface على الـ Router؟

Router > en  
 Router # Config T  
 Router(Config) # int F 0/1  
 Router(Config-if) # No Shutdown

③ في التكوين التالي، كيف يتم تكوين الـ Subinterface على الـ Router؟

Router(Config) # int F 0/1 ...

vlan 10 - 9

Router(Config) # int F 0/1 . 10 ...

Router(Config-Subif) # encapsulation dot 1 10 ...

Router(Config-Subif) # ip address ...

vlan 20 - 8

Router(Config) # int F 0/1 . 20 ...

Router(Config-Subif) # encapsulation dot 1 20 ...

Router(Config-Subif) # ip address ...

Show Ip Route. ————— Configuration

④ Layer 3 Switch

يتميز الـ Layer 3 Switch بأنه يعمل كـ Router و Switch و Bridge في آن واحد.

Plans ← gateway

Switch

Plan 1 ← 2 ← 3 ← 4 ← 5 ← 6 ← 7 ← 8 ← 9 ← 10 ← 11 ← 12 ← 13 ← 14 ← 15 ← 16 ← 17 ← 18 ← 19 ← 20 ← 21 ← 22 ← 23 ← 24 ← 25 ← 26 ← 27 ← 28 ← 29 ← 30 ← 31 ← 32 ← 33 ← 34 ← 35 ← 36 ← 37 ← 38 ← 39 ← 40 ← 41 ← 42 ← 43 ← 44 ← 45 ← 46 ← 47 ← 48 ← 49 ← 50 ← 51 ← 52 ← 53 ← 54 ← 55 ← 56 ← 57 ← 58 ← 59 ← 60 ← 61 ← 62 ← 63 ← 64 ← 65 ← 66 ← 67 ← 68 ← 69 ← 70 ← 71 ← 72 ← 73 ← 74 ← 75 ← 76 ← 77 ← 78 ← 79 ← 80 ← 81 ← 82 ← 83 ← 84 ← 85 ← 86 ← 87 ← 88 ← 89 ← 90 ← 91 ← 92 ← 93 ← 94 ← 95 ← 96 ← 97 ← 98 ← 99 ← 100

Router (config) # int E0/1

Switch Router (config) # no switchport

Switch Router (config) # ip address 192.168.1.1

Plans 1 ← 2 ← 3 ← 4 ← 5 ← 6 ← 7 ← 8 ← 9 ← 10 ← 11 ← 12 ← 13 ← 14 ← 15 ← 16 ← 17 ← 18 ← 19 ← 20 ← 21 ← 22 ← 23 ← 24 ← 25 ← 26 ← 27 ← 28 ← 29 ← 30 ← 31 ← 32 ← 33 ← 34 ← 35 ← 36 ← 37 ← 38 ← 39 ← 40 ← 41 ← 42 ← 43 ← 44 ← 45 ← 46 ← 47 ← 48 ← 49 ← 50 ← 51 ← 52 ← 53 ← 54 ← 55 ← 56 ← 57 ← 58 ← 59 ← 60 ← 61 ← 62 ← 63 ← 64 ← 65 ← 66 ← 67 ← 68 ← 69 ← 70 ← 71 ← 72 ← 73 ← 74 ← 75 ← 76 ← 77 ← 78 ← 79 ← 80 ← 81 ← 82 ← 83 ← 84 ← 85 ← 86 ← 87 ← 88 ← 89 ← 90 ← 91 ← 92 ← 93 ← 94 ← 95 ← 96 ← 97 ← 98 ← 99 ← 100

Switch Router (config) # interface vlan 1

Switch Router (config) # no shutdown

Switch Router (config) # ip address 192.168.1.1

Plans 1 ← 2 ← 3 ← 4 ← 5 ← 6 ← 7 ← 8 ← 9 ← 10 ← 11 ← 12 ← 13 ← 14 ← 15 ← 16 ← 17 ← 18 ← 19 ← 20 ← 21 ← 22 ← 23 ← 24 ← 25 ← 26 ← 27 ← 28 ← 29 ← 30 ← 31 ← 32 ← 33 ← 34 ← 35 ← 36 ← 37 ← 38 ← 39 ← 40 ← 41 ← 42 ← 43 ← 44 ← 45 ← 46 ← 47 ← 48 ← 49 ← 50 ← 51 ← 52 ← 53 ← 54 ← 55 ← 56 ← 57 ← 58 ← 59 ← 60 ← 61 ← 62 ← 63 ← 64 ← 65 ← 66 ← 67 ← 68 ← 69 ← 70 ← 71 ← 72 ← 73 ← 74 ← 75 ← 76 ← 77 ← 78 ← 79 ← 80 ← 81 ← 82 ← 83 ← 84 ← 85 ← 86 ← 87 ← 88 ← 89 ← 90 ← 91 ← 92 ← 93 ← 94 ← 95 ← 96 ← 97 ← 98 ← 99 ← 100

Layer 2 Switch Routing 192.168.1.1

Switch (config) # ip Routing

gateway 192.168.1.1

## Route Types

Dynamic

Static

Static Route III

في كبريا مشكلات حرجية و يجب ان تكون الحرجية كالتالي

1- لا يمكن الوصول الى الشبكة 2- التراما



الترتيب في الذاكرة هو Static Dynamic

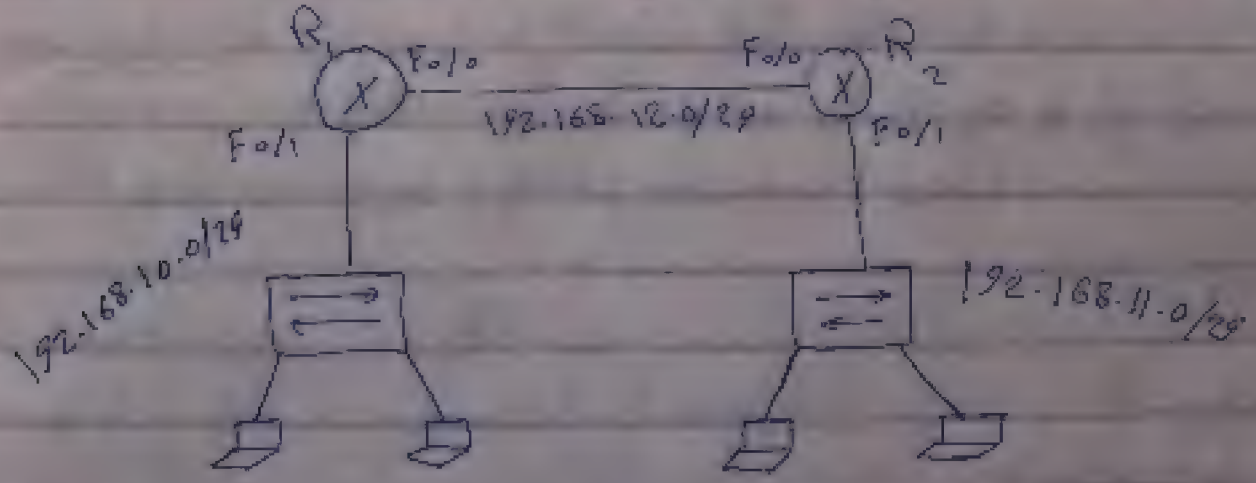
في الذاكرة static يظهر حرف S في اولها والـ Dynamic يظهر حرف D في اولها  
 في الذاكرة static يظهر حرف S في اولها والـ Dynamic يظهر حرف D في اولها  
 في الذاكرة static يظهر حرف S في اولها والـ Dynamic يظهر حرف D في اولها

## Static Configuration #

ننقل على الراوتر و نحدد الشبكة التي نريد تعريفها اليها و نكتبها في الذاكرة static  
 اتصال مباشر و نقوم بتعريفها في الذاكرة static

Router(config)# Ip Route 192.168.10.0/24 192.168.11.0/24

مثال لدينا جهازين راوتر R1 و R2 كل منهما شبكة لعناوينه مكانا الرسم  
 و الشبكة بين الراوترين مكانا الرسم كيف نعرفها كل شبكة متصلة على راوتر للجهاز الآخر  
 كل نوع الاتصال بين الشبكات مع طريقة استخدام الـ Static Route



الاجابة

في امكانك تعريف كل شبكة و تعطيل و تفعيل و حصر الـ IP التي يجب ان يكون  
 المتصل بالشبكة من كل راوتر و نستطيع ان نعرف كل جهاز في الشبكة الخاصة

هذا المخطط يبين الراوترات المتصلة في شبكة IP مع الشبكة بين الراوترات  
 سيكون لدينا مخرج كل راوتر على النحو التالي

R<sub>1</sub>

Fo/0 = 192.168.12.1/29

Fo/1 = 192.168.10.1/29 → وهو يمتد على الشبكة بأكملها

R<sub>2</sub>

Fo/0 = 192.168.12.2/29

Fo/1 = 192.168.11.1/29 → وهو يمتد على الشبكة بأكملها

(F) تجعل الـ static Route

R<sub>1</sub> الراوتر (P)

R<sub>1</sub>>en

R<sub>1</sub># Config T

R<sub>1</sub>(config)# Ip Route 192.168.11.0 255.255.255.0 Fo/0

↓  
Route

↓  
الشبكة المراد توجيهها للراوتر

↓  
المخرج الذي عليه  
خريطة فصل الشبكة

\* تليها أيضا اتصال اسم المخرج جيران الـ IP الخاص به

R<sub>1</sub>(config)# Ip Route 192.168.11.0 255.255.255.0 192.168.12.1

← IP الخاص بالجيران Fo/0 بدل كتابة اسم البورت

R<sub>2</sub> (N) الراوتر

R<sub>2</sub>>en

R<sub>2</sub># Config T

R<sub>2</sub>(config)# Ip Route 192.168.10.0 255.255.255.0 Fo/0

← أمر الراوتر

البورت الذي فصل  
منه الشبكة المراد توجيهها



# Configuring Static Routes - Example 1

R1 # Show IP Route

معرفة

C 192.168.10.0/24

Connected

C 192.168.12.0/24

Connected

S 192.168.11.0/24

Static

Connected هي الشبكات المتصلة بالراوتر مباشرة.

Static الشبكات التي لم يتم توصيلها بالراوتر عبر طريق Static Route.

R2 # Show IP Route

C 192.168.11.0/24

Connected

C 192.168.12.0/24

Connected

S 192.168.10.0/24

Static

وقد انك لاحظت في المخرجات التالية.

# لا نحتاج الى Static Route في هذه المخرجات

R2(Config) # No IP Route

# خاصية ال Default Route

نحتاج الى Static Route لاننا نحتاج الى الشبكات المراد توصيلها بالراوتر ولكن فرق

الراوتر انه لا يحتاج الى الوصول اليه عبر البورت بطريقة معينة

مثال

R1(Config) # IP Route 0.0.0.0 0.0.0.0 F0/0

من هنا اننا نحتاج الى ف0/0 لاننا نحتاج الى البورت F0/0 او يمكننا ان نكتب اليه  
بواسطة المخرج منه فالراوتر سيتصل بها Route وتسمى هذه الطريقة

ال Default Route

## # next hop

لدينا هنا اسم الـ next hop أو عنوان الـ IP الخاص به الذي نريد الوصول إليه  
الذي نكتبه عليه الـ Configuration هذا الـ next hop الـ exit port الذي يخرج  
منه البيانات

next hop هو الـ next hop المقابل من الراوتر الآخر الذي يصل به الـ next hop الذي  
نقل عليه الـ Config ونضع اسم الـ next hop عليه الـ config

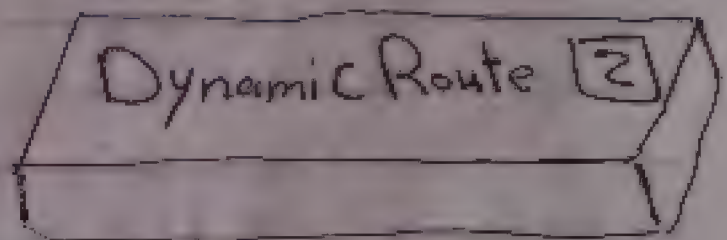
مثال

R1 (config) # ip route 192.168.11.0 255.255.255.0 192.168.12.1

هذا هو الـ exit port للراوتر R1 نكتبه عليه الـ next hop المقابل له من الجهاز R2 ليكون الأمر

R1 (config) # ip route 192.168.11.0 255.255.255.0 192.168.12.2

هذا هو عنوان الـ IP لـ next hop



هو استخدام البروتوكولات في عملية الـ Routing

يقوم الـ Dynamic Routing بعملية استطلاع الشبكات من أجهزة الراوتر المجاورة  
عن طريق Hello advertising

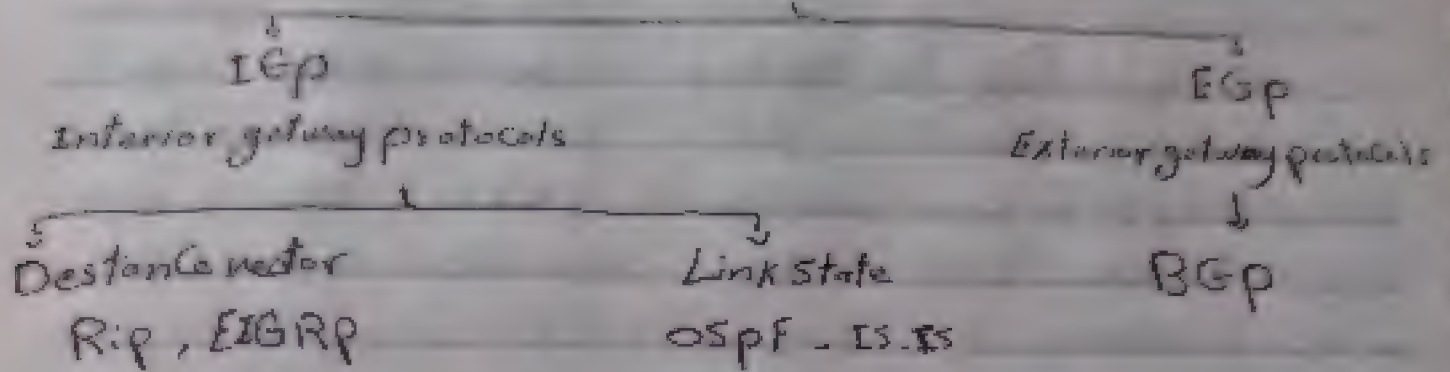
الـ Hello هو يقوم الراوتر بإرسالها لحزمة الأجهزة التي تستخدم نفس  
البروتوكول. ويتم الرد من الراوتر التي تستخدم نفس البروتوكول

الـ advertising عند التعرف على الأجهزة التي تستخدم نفس البروتوكول

يقوم كل جهاز بإعلام الجيران الآخرين بـ Routing table الخاصة به



# Routing protocols #

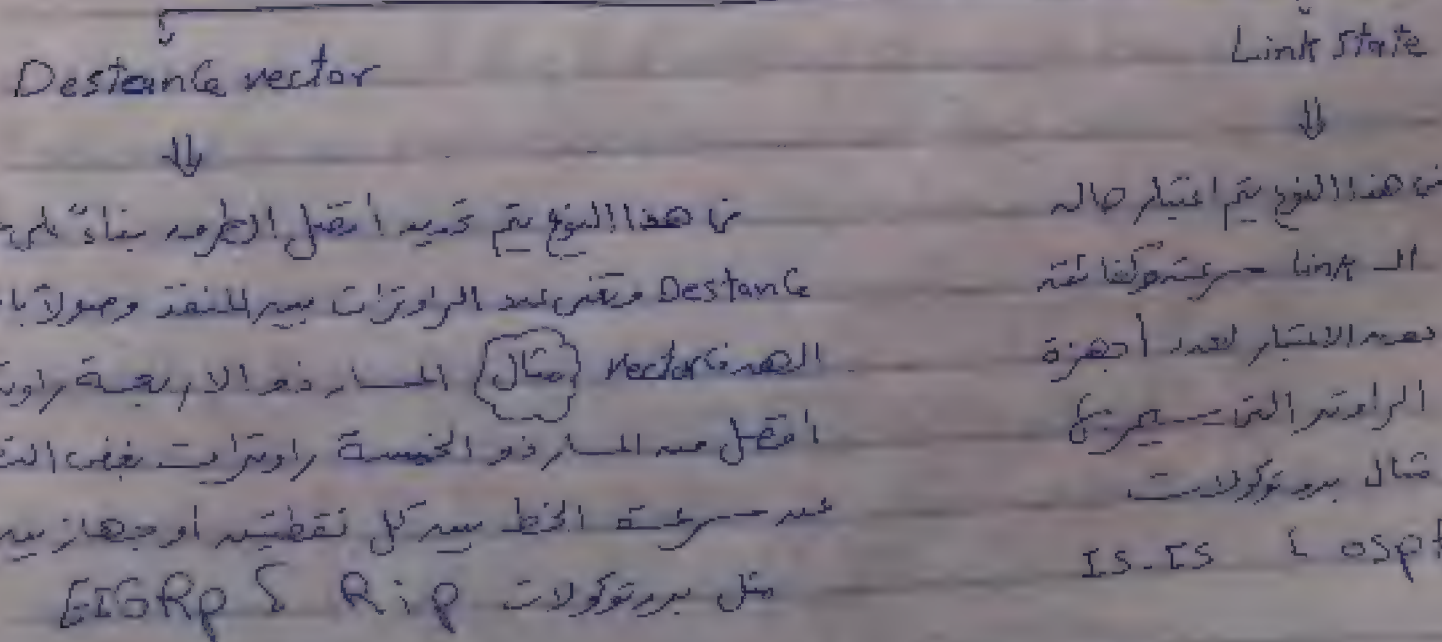


تنقسم الـ Routing protocols كما في الرسم التالي:

① Interior : هي داخلية [Rip, ospf, EIGRP] وهي العملية فيها مجال عمل واحد كما في شبكة الواحدة أو شبكة الواحدة - شبكة الواحدة - شبكة الواحدة

② Exterior : هي خارجية [BGP] تعمل بين مجال عمل منفصلين ما يعرف بـ Autonomous systems، الأنظمة المستقلة، لأنه يعمل بين شبكتين أو شبكات منفصلة من بلد ما أو من منطقتين منفصلتين.

وتنقسم الـ Interior إلى:



## مقارنة بروتوكولات التوجيه

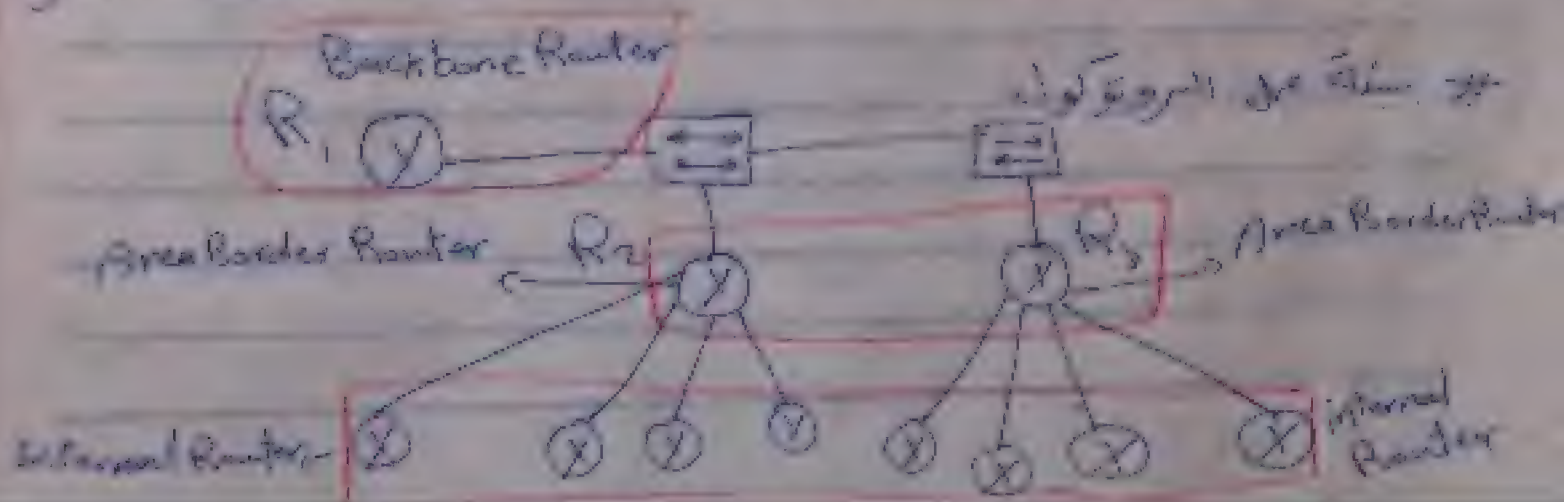
	Rip	Rip2	Eigrp	ospf	isis
VL5 on	No	yes	yes	yes	yes
Administrative distance	120	120	90	110	115
Algorithm	Dv	Dv	advanced dv	LS	LS
route summarization	No	yes	yes	yes	yes
Costs proprietary	No	No	yes	No	No
Max hop Count	15	15	255	infinite	

Administrative distance هي نسبة تقيسها البروتوكولات من المفاضلة بين الطرق حيث أن الأقل هي الأفضل  
 Cost هو عبارة عن عدد hops

max hop count هو كم أقص يمكن أن يصل إليه البروتوكول من hops

## ١) بروتوكول ospf

هو اختيار أول open shortest path first بين طرق أقصر مسار  
 كل مسارات الـ link state متقنة من شبكة المسيرة وتكون أكثر البروتوكولات  
 كفاءة وهو بروتوكول standard أو أنه يعمل على أجهزة سيسكو وغيرها من أجهزة





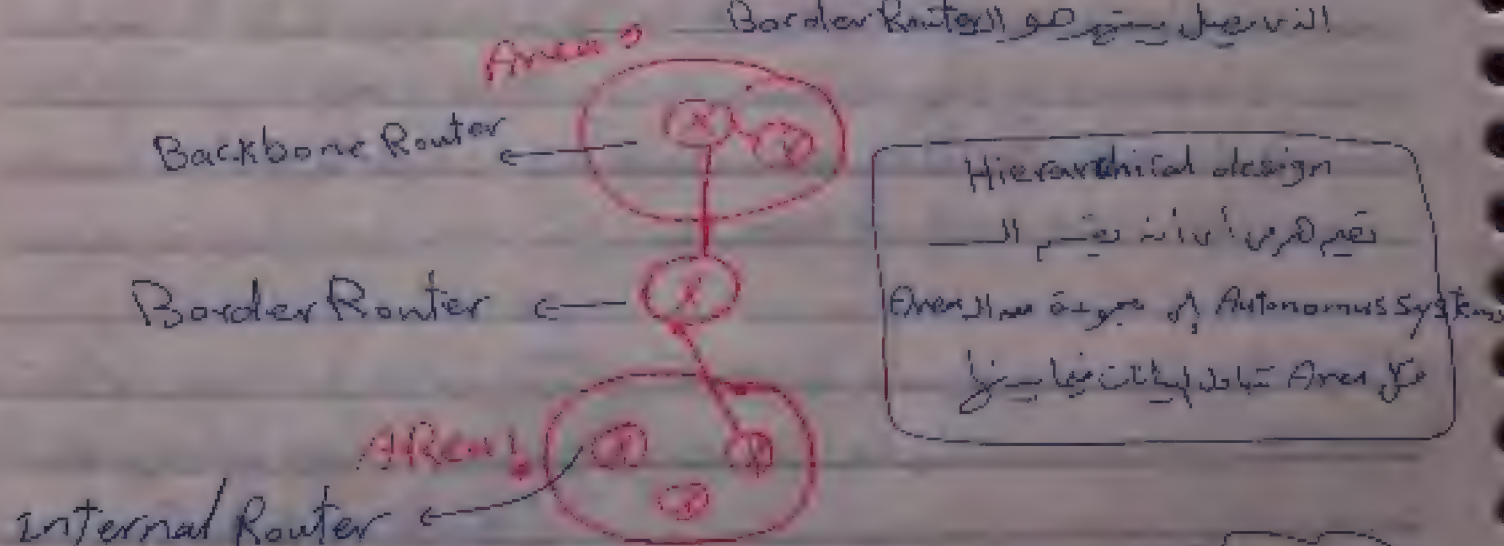
فإنها الروترة لا يتم تصميم الشبكة إلا في البداية

Area 0

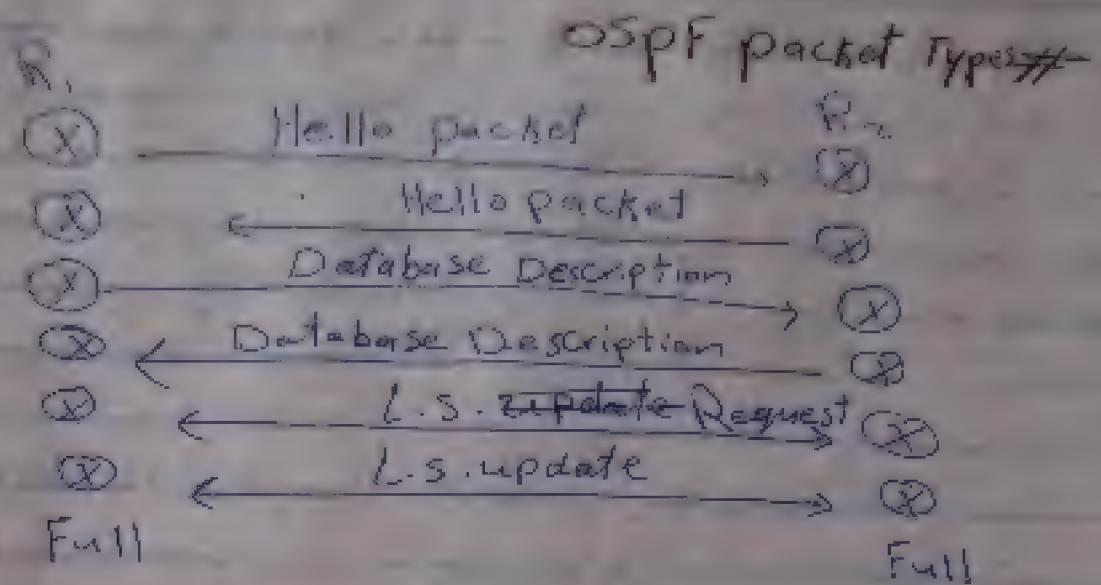
هذه هي Area 0، فهي عادةً تكون Backbone Area، وهي المنطقة التي  
تحتوي على جميع الروترة الأخرى، وهي المنطقة التي  
تحتوي على جميع الروترة الأخرى، وهي المنطقة التي  
تحتوي على جميع الروترة الأخرى، وهي المنطقة التي

② Internal Routers: هي الروترات الأخرى في المنطقة الأخرى مع ملاحظة  
أن كل منطقة لديها ٥٠٠ روتر فكلنا ٥٠٠ روتر في كلون  
Area مثل Area 1 في Area 0 كل الأجهزة في هذه Area متصلة أيضًا  
ببعضها

③ Border Router: هي الروترة التي تصل الأجهزة في Backbone Area  
في Area 0 بالروترات في Area 1 المختلفة الأخرى، هي الروترة  
التي تصل بين Area 0 و Border Router



فكرة العمل: فكرة عمل البروتوكول عمومًا هي إرسال رسالة Hello للقرن  
على الأجهزة التي تستخدم نفس البروتوكول بعد عملية التعرف كل جهاز  
يرسل Advertising عن نفسه الراوي في Table فيقوم كل جهاز بالمقارنة  
بالبقية على المعايير الخاصة بالبروتوكول، فكل جهاز هذا يوضحه فكرة العمل



يقوم كل جهاز بإرسال رسالة الـ Hello لمعرفة الأجهزة التي تستخدم البروتوكول  
 ؟ يقوم كل جهاز بإرسال LSA تحتوي على Database الخاصة به يقارن كل  
 راوتر بالـ Database الخاصة به ويتفق على إرسال LSA  
 Link state Request يطلب بياناته ويريد الحصول عليها من راوتر معين فيقوم الراوتر الآخر  
 بإرسال LSA يحتوي على الـ update للجزء المطلوب من الجهاز الآخر  
 وبالتالي ينقل الـ Routing table.

بالنسبة لـ LS Ack ترسل لتأكيد استلام أخلا البيانات المختلفة المستقبلة  
 والمرسله من المرسل والمستقبل وهذا اختصار Link state Acknowledgment

هنا عندما يصل الراوتر إلى Link state Database من يأتى من خوارزميات SpF  
 Short path First فيقوم بتفعيل السياسات وحساب أفضل المسارات من أجل الـ Table  
 التي تسمى "Routing Table"

## ospf Topology ##

بروتوكول ospf يقوم بإنشاء ثلاث جداول كل جدول له وظيفة محددة.

ospf Topology database ②

Neighbor Table ①

Routing Table ③



### 3 Dead Neighbors Table

يحتوي هذا الجدول على قائمة جيران OSPF الذين لم يتم تلقي تحديثاتهم في وقت معين. إذا لم يتم تلقي تحديثات الجيران في وقت معين، فإنهم يُدرجون في هذا الجدول. يتم تحديث هذا الجدول كل 30 ثانية. إذا لم يتم تلقي تحديثات الجيران في وقت معين، فإنهم يُدرجون في هذا الجدول.

Dead Table

Hellotime: اختبار الجيران. إذا لم يتم تلقي تحديثات الجيران في وقت معين، فإنهم يُدرجون في هذا الجدول.

Dead: الوقت الذي لا يتم تلقي تحديثات الجيران فيه. إذا لم يتم تلقي تحديثات الجيران في وقت معين، فإنهم يُدرجون في هذا الجدول.

من قائمة الجيران: 40 ثانية

Router # show ip ospf neighbors: قائمة الجيران عن طريق الأسماء

### 2 OSPF Topology Database

LSDB: قاعدة بيانات Topology Database. يُستخدم لجمع جميع البيانات من الجيران. يُستخدم لجمع جميع البيانات من الجيران.

Router # show ip ospf database

### 3 Routing Table

Forwarding database: قاعدة بيانات Forwarding database. يُستخدم لجمع جميع البيانات من الجيران. يُستخدم لجمع جميع البيانات من الجيران.

# show ip route [ospf]

## OSPF Configuration

### 1 Single Area Configuration

① تشغيل البروتوكول وتعيين رقم المنطقة

Router(Config) # Router ospf 1

الرقم المحدد هو البروتوكول

الرقم المحدد

$$\begin{array}{l} \text{100} \rightarrow 255.255.255.255 \\ \text{255} \rightarrow 255.255.255.255 \end{array}$$

Router(config-Router) # network 10.0.0.0 255.255.255.0

Single Area ISL and VLS Config

```
Router(Config)#Router ospf 1
```

## [2] Multi Area Configuration

المهمة للـ Config له صلاحيات مع Single أنه يمكن تشغيل الـ ospf على كل روتر من Areas المختلفة ونفرض على الـ شبكات المتصلة به وهذه طريقة LSA - تتغير على الـ شبكات الأخرى

معادله ۱:  $OSPF$  که به نام پروتکل مسیریابی در شبکه‌های محلی (LAN) شناخته می‌شود، یکی از پروتکل‌های مسیریابی در شبکه‌های محلی است.



أمرنا ادخل شبكة على جهازنا

Router(Config) # Router ospf 1

وبعد ذلك ادخل شبكة داخلنا ونقص الراوتر فإنا أدخلنا على نفس الشبكة

Router(Config) # Router ospf 1

وبعدنا أكتب الشبكة أو أنا بديل سراج أدخلنا تحت هذه الشبكة

## Router ID #

هو رقم ID خاص بالراوتر لا يتشابه مع غيره بين الراوترات في نفس Area ويتكون من

32 Bit وله نفس هيكلية ال IPv4

عند إرسال رسالة LSا تحتوي هذه الرسالة على معلومات من ضمنها Router ID

هناك طريقة للراوتر ID بعد طريقة

1- ألقاها بالأمر المباشر

(Config-if) # Router-id < ip address >

2- إذا لم تكن هذا الأمر - يتم اختيار Loopback IP address وهي عبارة عن بوردا

وهي تتكون من 32 Bit

3- إذا لم يتم اختيار Loopback IP address - يتم اختيار أول IP موجود في physical interface من الراوتر

باختصار Router ID

1- الأمر المباشر (أولاً)

2- أول Loopback IP (أولاً)

3- أول physical interface IP

\* يتم اختيار Router ID في عملية الانتخابات. لاختيار الراوتر الرئيس

# ID Configuration #

Router(Config) # Router-id < ip address >

Router(Config) # int loopback 0

(config-if) # ip address ip mask

(config-if) # no shut

● Router of class ip = ospf process  
 بعد اختيار الطريقة نكتبها الأمر  
 وذلك لتسمح الراوتر ليدرك المسارات التي يمكن استخدامها في المسار المستقبلي  
 ان لا يكون المسار الذي نختاره

## ospf metric #

المترية metric هو المعيار الذي نستخدمه لاختيار البروتوكول المسار المفضل  
 لتفويج البيانات .

عند الـ ospf على الـ Cost ويتم حساب الـ Cost عن طريق  
 المعادلة 
$$Cost = \frac{100000000}{Linkspeed}$$

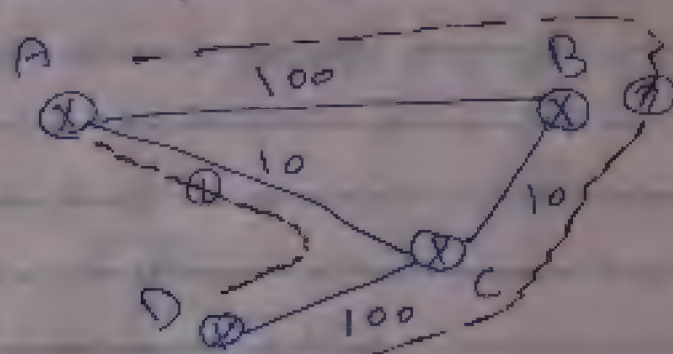
حيث  $10^8 \text{ Bit/s} = 100000000$  أو 100 ميغا

ولـ Linkspeed هو الـ Bandwidth بالـ Bits أو الميغا

فلو كانت الـ Link سرعة 10 ميغا :  $Cost = \frac{100}{10} = 10$

ولذلك الـ Link سرعة 100 ميغا :  $Cost = \frac{100}{100} = 1$

والمراد صاحب اقل تكلفة هو الذي يختاره البروتوكول في الـ Routing table



نلاحظ ان الراوتر A يصل الى الراوتر D به طريقه مباشرة هو 1  
 25

المسار رقم (1) نجد ان الـ Cost الاجمالي  $= \frac{100}{100} + \frac{100}{10} = 1 + 10 = 11$

المسار (2)  $= \frac{100}{100} + \frac{100}{10} + \frac{100}{100} = 1 + 10 + 1 = 12$

المسار رقم (3) اقل مسار حيث ان صاحب الـ Cost الاقل لذلك

هذا المسار هو الذي سيوضع في الـ Routing table واما المسار الاخر بالاضافه

للمسار (1) سيوضع في الـ Topology tables حيث انه وضع فيه جميع

المسارات المتوفرة الى الـ Destination



# كيفية تغيير مسار حركة المرور  
 لا يمكننا أن نغير مسار حركة المرور في OSPF إلا عن طريق تغيير الـ Cost من الـ Link أو الـ Interface  
 لذلك إذا قمنا بتغيير الـ Bandwidth في الـ Interface، فإن الـ Cost سيتغير تلقائياً  
 (تغيير الـ Cost مع سرعة حركة المرور)  
 (Config-IF) # ip ospf cost <no>

② تغيير الـ Bandwidth  
 (Config-IF) # bandwidth <no in Kbps>

③ تغيير الـ Reference Cost  
 نلاحظ أن الـ Reference Cost هو الـ Cost الخاص به هو (1) نلاحظ  
 أنه الـ Cost لا يتغير، ولكن الـ Bandwidth يتغير، حيث أن الـ Bandwidth يتغير  
 $\frac{1}{10} = \frac{100}{1000}$  حيث أن الـ Cost لا يتغير، ولكن الـ Bandwidth يتغير  
 الـ Reference Cost = 1000، لذلك نلاحظ أن الـ Reference Cost = 10  
 نلاحظ أن الـ Reference Cost = 1000، لذلك نلاحظ أن الـ Reference Cost = 10  
 نلاحظ أن الـ Reference Cost = 1000، لذلك نلاحظ أن الـ Reference Cost = 10  
 نلاحظ أن الـ Reference Cost = 1000، لذلك نلاحظ أن الـ Reference Cost = 10

Router(Config-Router) # ospf auto-cost Reference-bandwidth <no>

# Load Balancing

لا يمكننا أن نغير مسار حركة المرور في OSPF إلا عن طريق تغيير الـ Cost من الـ Link أو الـ Interface  
 لذلك إذا قمنا بتغيير الـ Bandwidth في الـ Interface، فإن الـ Cost سيتغير تلقائياً  
 (تغيير الـ Cost مع سرعة حركة المرور)  
 (Config-IF) # ip ospf cost <no>

Router(Config-Router) # maximum-path <no>

# OSPF Network Types

نوع 1: Point-to-Point (نوع 1) هو شبكة التي يتصل بها رابط واحد فقط



Point-to-Point (1)

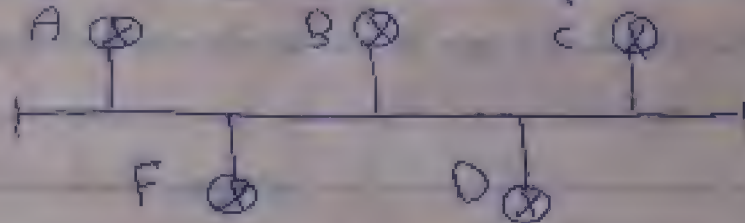
وهو يتكون من رابطتين فقط، أي رابطتين متصلتين مع بعضهما البعض، حيث يتم نقل البيانات من رابط HDLC أو PPP إلى رابط الآخر، حيث يتم نقل البيانات من رابط HDLC أو PPP إلى رابط الآخر.

Non Broadcast multi Access (2)

هو شبكة ليس فيها القدرة على نقل Broadcast، وتحتاج Config خاصة للتحقق من أن neighbors هي في شبكة.

Broadcast multi Access (3)

هو شبكة فيها أكثر من رابطتين، حيث يتم إرسال Broadcast وتلك multiCast يكون فيها جهاز رئيس يسمى Designated Router (DR) وجهاز نائب له وهو Backup Designated Router (BDR) والباقي يسمى DR (Designated Router) وتسمى الـ Loop (Loop) الاختيار هو تقليل عدد الـ Loop وكنتم أنه يجب أن يكون Loop.



مثال

عند إرسال Hello packet من الجهاز A سيصل إلى B، C، D، F  
 F - D - C - A ~ ~ B ~ ~ ~ ~  
 F - D - B - A ~ ~ C ~ ~ ~ ~  
 F - C - B - A ~ ~ D ~ ~ ~ ~  
 D - C - B - A ~ ~ F ~ ~ ~ ~

عند جهاز يرسل لكل الأجهزة تلك عند صحت، إرسال LSA أو خلاصة الـ LSA لكل الأجهزة من حيث عملية الـ Loop



صحة جهاز A مثل إرسال update لكل الأجهزة التي تتصلقاتها  
 مرة أخرى لكل الأجهزة وبالنسبة لغيرها لا شيء وانترية منه ارسال البيانات  
 لذلك كان لكل من انتظاما رئيس ومضيف رئيس يتم ارسال الـ LSA  
 اليهما ويقوم الرئيس بارسال الـ LSA إلى الأجهزة الأخرى والمضيف  
 يستلم الأجهزة الأخرى لا يرسل الـ Backup  
 (مثال) من المثال السابق نلاحظ ان جهاز A هو الـ DR و B و C و D هم الـ BDR  
 إذا كان C يرسل LSA فينتقل إلى A و B و D  
 A هو الـ DR و B هو الـ BDR و C و D هم الـ DROthers  
 Loop

### ٣- كيفية اختيار الـ DR و BDR

(أ) يتم اختيار الـ DR ونائبه BDR على أساس الـ interface صاحب  
 أعلى قيمة priority أولوية والـ priority رقم مكوّن من 0 إلى 255  
 صفر إلى 255 وتكون الـ default priority (1) وتكون القيمة  
 router (config) # int E0/0

Router (config) # ip ospf priority (no)

مع ملاحظة أنه الرقم لكان صفر فهذا معناه أنه الـ interface له تكون الـ DR  
 أو BDR وكذلك ليس معناه أنه interface هو الـ DR فهو مخصص أنه تكون كل  
 البورتات من هذا الراوتر الـ DR بل كل شبكة مستقلة تستطيع الـ DR من البورتات  
 من هذه الـ Topology

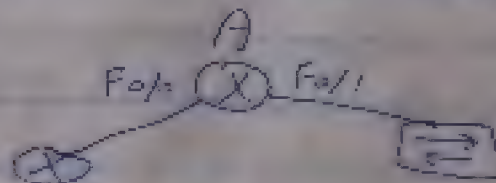
(ب) إذا كانت جميع الـ priority متساوية يتم اختيار صاحب الـ Router ID  
 ليكون هو الـ DR ونائبه الذي يليه

مع ملاحظة أنه إذا لم يتم تعيين الـ priority للمرئيه له تكون  
 الـ DR لأنه لا يتم الانتخاب سوى مرة واحدة كانه إذا سقط الـ DR  
 أو قتل لم يكن مدة الـ Dead time نائبه يكون الـ DR ونائب اختيار الـ BDR

- الاختلافات بين OSPF و RIPv2 هي:
  - 1- RIPv2 هو بروتوكول مسطح (flat) بينما OSPF هو بروتوكول هرمي (hierarchical).
  - 2- RIPv2 هو بروتوكول مسطح (flat) بينما OSPF هو بروتوكول هرمي (hierarchical).

## passive interface

عند تفعيل الواجهة على البورت - سوف يتلقى هيلو باكيت



النتيجة

من هذا الشكل البورت Fa0/1 متصل بمسويين فلا حاجة الى ال hello packet عليه لأنه ذلك سيصله من CPU الخاص بالمرور لذلك فلا حاجة الى ال hello packet من ال Fa0/1.   
 من ناحية أخرى، لكي يصل ال hello packet الى ال Fa0/1، يجب ان يكون ال CPU متصلاً بالمرور.   
 لكن تفعيل ال hello packet على البورت سيؤدي ذلك الى توفير ال hello packet الى ال CPU.

Router (config) # Router ospf F ---

Router (config - Router) # passive interface 0/1

ولذلك لن يرسل ال hello packet الى ال CPU.

No passive interface F ---

• من ناحية أخرى، لكي يصل ال hello packet الى ال Fa0/1، يجب ان يكون ال CPU متصلاً بالمرور.   
 • من ناحية أخرى، لكي يصل ال hello packet الى ال Fa0/1، يجب ان يكون ال CPU متصلاً بالمرور.

## # خلاصة ال ospf Config #

### ① Basic ospf

Router (config) # Router ospf 1 ex

Router (config - Router) # network IP + wildcard + Area



### [2] Router ID

Router (Config-Router) # Router ID no  
Loopback Router (Config) # int loopback no  
Router (config-if) # ip address no  
Router # clear ip ospf process

### [3] priority

Router (Config) # int no  
Router (config-if) # ip ospf priority no

### [4] Cost

Router (Config) # int no  
Router (config-if) # ip ospf cost no  
Router (config-if) # bandwidth no in kbps  
Router (Config-Router) # ospf auto-reference bandwidth no

### [5] cost per interface

Router (Config-Router) # maximum-path no

### [6] Hello Interval

(Config-if) # ip ospf hello-interval no in sec  
(Config-if) # ip ospf dead-interval no in sec

### [7] Show Commands

show ip protocols	معلومات البروتوكول	show ip ospf neighbors	جيران
show ip route ospf	مسارات OSPF	show ip ospf process	عملية
show ip ospf interface	واجهة OSPF	show ip ospf database	قاعدة بيانات
show ip ospf	LSA	Routing Table	جدول التوجيه
		Router # clear ip route	

# EIGRP protocol

هو بروتوكول Interior Gateway Routing Protocol (IGRP) من شركة Cisco proprietary. وهو بروتوكول ذاتي الجذر. يستخدم Distance vector routing protocol EIGRP وهو بروتوكول Distance vector.

## مميزات

- 1- سهولة الإعداد حيث أنه لا يتطلب جبهة كبيرة.
- 2- البروتوكول الوحيد الذي يمكنه مسار اختيار حيث يقلل الجهد على مسار اختياره في Topology إذا فقد المسار الأساسي.
- 3- الـ Summarization يمكنه عليه تلقائياً وعلى إيقافه عبر الجبهة Auto-Summary.
- 4- غير البروتوكولات - اعتماداً على مخرج الـ Routing.
- 5- بروتوكول hybrid يجمع بين Distance vector وقوة الـ Link stat.

## عيوبه

- 1- يعمل مع أجهزة سيكو فقط.
- 2- عدم القدرة على حساب الـ metric.

## جداول EIGRP

بروتوكول EIGRP يقوم أنشأ 3 جداول

① Neighbor Table : ويحتوي على معلومات جميع الجيران في الشبكة ويظهر بالأمر

# show ip eigrp neighbor

② Topology Table : يستخدم لمعرفة أفضل مسار Successor ، كما نلاحظ على مسار

Feasible Successor ويظهر بالأمر # show ip eigrp topology

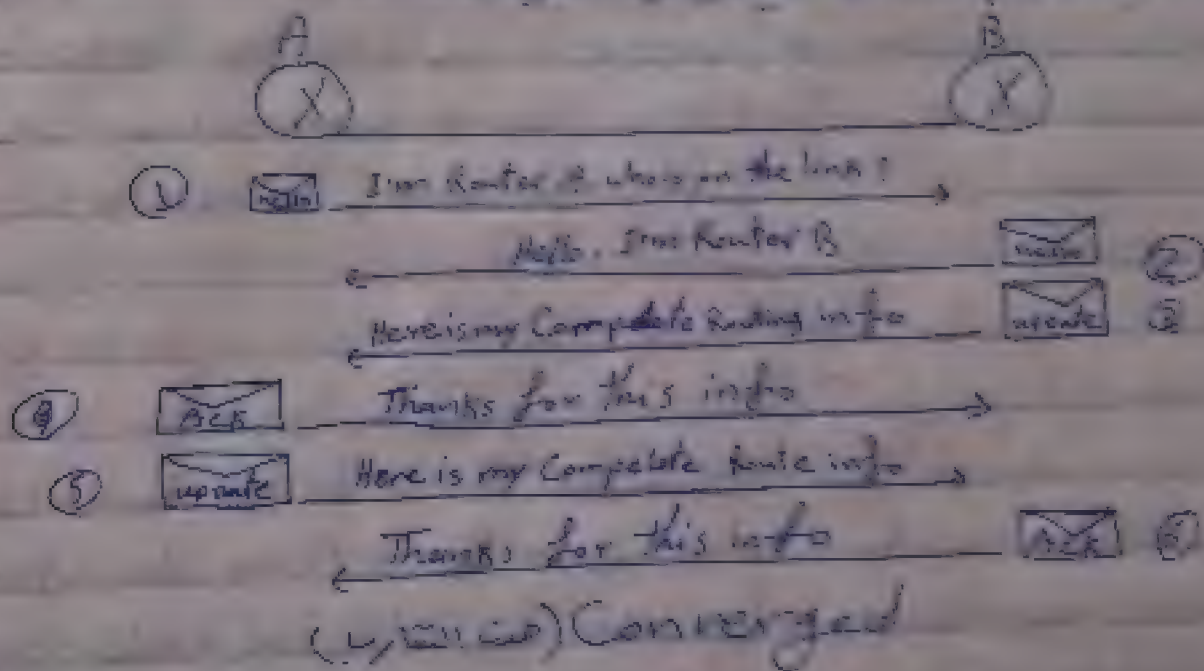
③ Routing Table : لمعرفة أفضل مسار في الـ Routing ويظهر

بالأمر # show ip route



## استاد هندسة مع الشبكات

يتم تعريفه بأنه النوع من خوارزميات استناد على معلومات مع جيرانه فكلما أتيحت  
 له معلومات إضافية، كلما تحسن في تقديم الروابط الأفضل *Feasible Successor*  
 يقوم الروابط التي تعتبر بأنها أفضل من تلك التي هي موجودة *multi cost* من جيرانه إلى جيرانه  
 وتتميز الروابط بأنها لا تحتاج إلى شكل التكاليف  
 ① *hello packet* → للتحقق من الروابط والأجهزة  
 ② *update packet* → إرسال معلومات وتحديثات إلى *Routers*  
 ③ *Query packet* → إذا كان هناك تغيير في المسار أو تغيير في تقسيم المسار الأصلي  
 ④ *Reply packet* → في حالة *Query* المرسل من نظام المرسل إلى المرسل بالمراسلة الاحتياطية  
 ⑤ *Ack packet* → تأكيد استلام المعلومات



من حيث المعلومات بين الروابط يأتي تحت المراتب الرئيسية والمسارات  
 الاحتياطية *Successor* و *Feasible Successor*  
 ويتم تصنيف المسارات من طرف حساب *Advertised distance* و *Feasible distance*

① *Advertised distance* → المسافة بين الراوتر المجاور وبينه الوجهة الرئيسية  
 ② *Feasible distance* → المسافة الكلية بينه وبينه الوجهة الرئيسية  
 مثال: إذا كان *AD* المسافة بين الراوتر المجاور والوجهة الرئيسية

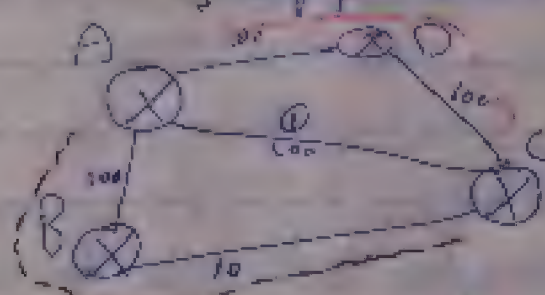


مثال

إذا كان A يقصد الوصول إلى C فإنه أفضل مسار هو المسار Successor  
والمسار ليس Feasible Successor حيث أنه لا Advertised distance من A إلى C  
من المسار للوجه التالي وهو من B إلى C بينما Advertised distance من  
المسار إلى C = المسار من A إلى B + المسار من B إلى C

# تحديد ال Successor & Feasible Successor

ال Successor هو المسار صاحب أقل تكلفة  
ال Feasible Successor هو المسار الذي يملك صاحب ثاني أقل تكلفة لكنه هناك  
شرط صحت يكون Feasible Suc. وهو أن تكون ال Advertised Distance من هذا المسار  
أقل من ال Feasible Distance من المسار الرئيس "ال Successor" هذا  
الشرط يسمى ال Feasible Condition والعرض الرئيس من هذه القاعدة  
هو منع عملية الدوران "Loop prevention"



مثال

باعتبار أن المسار رقم ①

هو أفضل مسار من B إلى A سيكون هناك مسار من A حيث الوصول من طريق  
الرافعة D وطريق الرافعة B لذلك يتم اختيار ال Feasible Successor  
من خلال المسار الذي فيه Advertised distance أقل من التكلفة الكلية للمسار ①  
فبفرض أن Ad من المسار B هو 10 و Ad من المسار D هو 100  
المسار الذي فيه Ad أقل من التكلفة الكلية للمسار الرئيس هو B من المسار  
هو ال Feasible Successor

# EIGRP Metric

ال metric الخاص بهذا البروتوكول معقد نوعاً ما فهو يعتمد على خمس قيم  
وهي Bandwidth (K1) Delay (K2) Reliability (K3 & K5) Load (K4)



مقياس  $K_2 \leq K_1$   $K_3 \leq K_2$   $K_4 \leq K_3$

مقياس  $\alpha$  metric المقدم

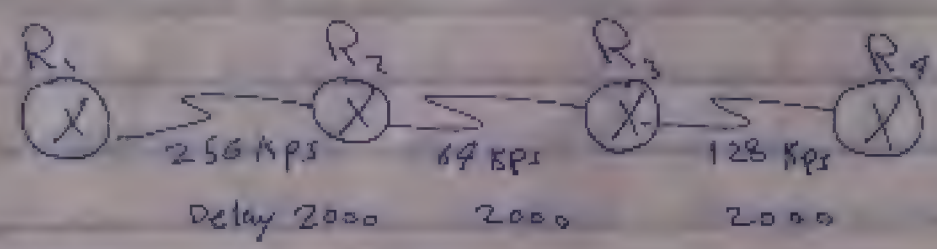
$$metric = 256 \times (Bandwidth + Delay)$$

① الناحية Bandwidth: وهي عبارة عن سرعة موزونة بين الـ Source والـ Destination

$$Bandwidth = \frac{10^7}{\text{least bandwidth in Kps}}$$

وهي  $\frac{10^7}{\text{أقل سرعة في الكابلات الموصلة للوجهة المطلوبة}}$

② التأخير Delay: وهي عبارة عن مقدار التأخير الذي يسبب في الوصول من المصدر إلى الوجهة النهائية. أي أنها التأخير في الكابلات



نلاحظ أنه سرعة الكابل بين  $R_2$  و  $R_3$  هو 64 Kps وهو أصغر أقل Bandwidth لذلك هو الذي سيؤثر في الـ Delay لأننا نأخذ القيمة 2000 بين  $R_2$  و  $R_3$  فقط.

$$metric = 256 \left( \frac{10^7}{64 Kps} + 2000 + 2000 + 2000 \right)$$

$$metric = 256 \times (156250 + 2000 + 2000 + 2000)$$

$$metric = 256 \times (156250 + 6000)$$

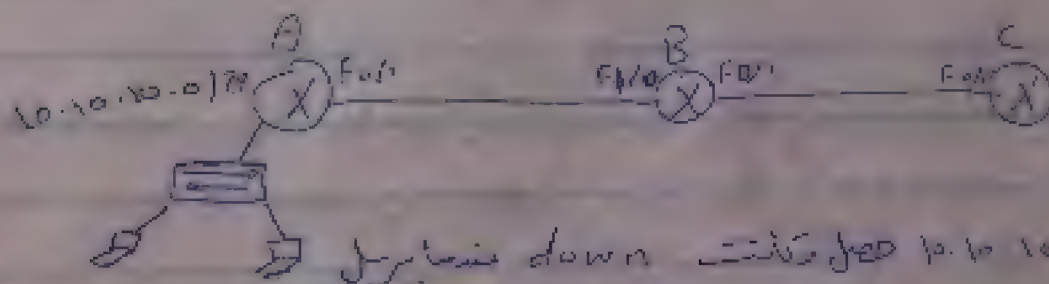
$$metric = 256 \times 162250$$

$$metric = 41536000$$

في البداية يتم تحديث الجداول في كل Router  
 ثم يتم إرسال التحديثات إلى الجداول في routers المجاورة  
 المتصلة بالخطوط

• يمكن استخدام Diffusing update algorithm  
 Diffusing update algorithm هو آلية اختيار المسار الرئيسي والاحتياط  
 عند استخدام آليات تحديثات المسار في حالة فشل المسار الرئيسي  
 حيث يتم اختيار المسار الاحتياطي في حالة فشل المسار الرئيسي

## # مشكلة الـ Routing Loops



(1)

في حالة فشل المسار الرئيسي يتم إرسال التحديثات إلى المسار الاحتياطي  
 update للوقت الأخرى يرسلها بعد 30 ثانية فإذا أرسل B قبل أن  
 يرسل A update فإنه A سيقبل أنه هناك مسار جديد له شبكة 10.10.10.1  
 وبالتالي سيحل محل المسار القديم في Table المسار على A update المستلمة من B  
 ثم يرسل A update لـ B فيجاءه هناك شبكة 10.10.10.1 مساراً جديداً  
 A فيجاءه B update فقلنا كيف يمكن تجنب ذلك؟



لحل هذه المشكلة نستخدم Routing Loop ويمكن التخلص منه بالطرق التالية:

- 1. max hop count
- 2. Route poisoning
- 3. Triggered update
- 4. Split Horizon
- 5. Hold down timers



④ Hold down timer  
تتمثل في وقت لا يقل عن 30 ثانية بعد تلقي رسالة update من الجارة المجاورة



تتمثل في وقت لا يقل عن 30 ثانية بعد تلقي رسالة update من الجارة المجاورة  
بشكل دوري أو عند حدوث تغيير في حالة الشبكة

### Split horizon ⑤

تتمثل في منع إرسال المعلومة إلى مصدر المعلومة من آخر لها. إرسال update من B إلى A يتم منع إرسال update من A إلى B حيث أن A هو الذي علم B عن طريق Loop وبالتالي لا يتم إرسال update إلى B عن طريق B. هذا

### Route poisoning ⑥

تتمثل في إعلان حالة الفشل إذا الراوتر وجد أنه هناك شبكة معينة أصبحت غير موجودة. يتم إعلان Route poisoning أن يعتبر الشبكة هذه على بعد 16 راوتر أو مسار أو أكثر. next hops آخرها 16 فبالنظر إلى الشبكة غير موجودة بدلاً من انتظار 30 ثانية إلى update من الراوترات 16 مرة لا يعرفون أن الشبكة على بعد 16 مسار في حلولة غير موجودة.

### Triggered update ⑦

هذه الخطوة يتم على الراوتر إرسال update مباشرة فحالة أنه شبكة تكونت عند إعلان تغييره على مدة الانتظار P interval time ثم لا يدخل Loop

### Hold down timers ⑧

هذه الميزة تمنع الراوتر من أن لا يتغير مفهوم مباشرة بل ينتظر فترة زمنية ثم يتغير آخر update وحالها. هذا أن مفهومه أنه غير موجود لكنه لو وجد المسار سيظل أنه موجود.

# Load Balancing Example #

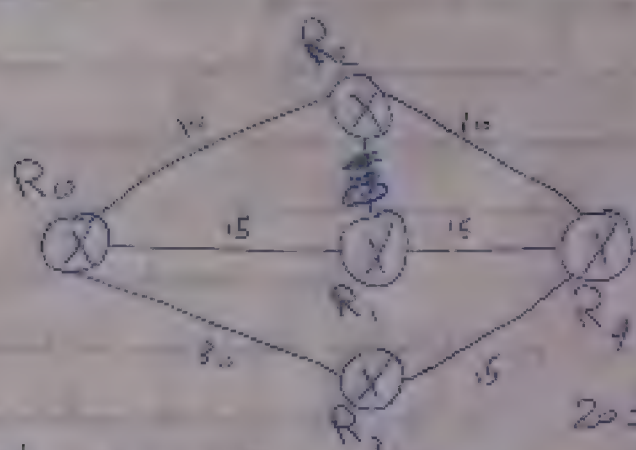
Load Balancing هو توزيع الحمل على عدة خوادم لتوزيع العمل وتقليل الضغط على الخادم الواحد.  
الهدف من Load Balancing هو توزيع الحمل على عدة خوادم لتوزيع العمل وتقليل الضغط على الخادم الواحد.  
الهدف من Load Balancing هو توزيع الحمل على عدة خوادم لتوزيع العمل وتقليل الضغط على الخادم الواحد.

111. *Exilis*

Copy!

اشعار - حیدر علی خان -  
میں نے تم کو فراموش کر دیا

تغير مع ما يكون المميزات لهذه المقترحات



is equal to  $\frac{1}{2}$



کما مررت به لسان

من  $R_0$  إلى  $R_1$  حيث  $\alpha = 2$

والناتجة  $R_0 \rightarrow R_1 \rightarrow R_2 \rightarrow \dots$  هي المسار الاعتيادي حيث  $R_0$  هو صاحب أقل metric

في حين اننا نستخدم عبارات غير متداوية مثل نقل الـ Traffic الى الـ Destination  
عبر طريق معين الى الـ server فكل هذا هو الـ metric = 1 - مثلا الى الـ metric  
 $= 1 \times 20 = 20$  (المسار الرئيسي) والاصغر هو 30 بفرض اننا في  
الـ warm up يكون الـ metric = 28 و الـ 20 في المسار الرئيسي = 70  
او سبع مرات تكرر ذلك او متساوي في المستمرة من الـ Load Balancing  
وهذا المسار الاصغر = 3 وهو اقل من الـ 28 فبالاخره سيتم الـ Load Balancing  
بالتساوي بين الـ metric الى المسار الرئيسي.



## EIGRP Configuration

Router (config) # Router EIGRP AS number

Router (config-router) # network IP

Router (config-router) # no auto-summary

show ip

Router # show ip route

Router # show ip route eigrp

Router # show ip eigrp neighbors

Router # show ip eigrp topology

variable ~~name~~

Router (config) # Router eigrp AS number

Router (config-router) # variable name

passive

Router (config-router) # passive interface F0/0

maximum

Router (config-router) # maximum path count

الوقت

Router (config) # F 0/0

Router (config-if) # ip hello-interval eigrp seconds

Router (config-if) # ip hold-interval eigrp seconds

hold Hello seconds Hello seconds Hold seconds  
Hello seconds

Router # clear ip route

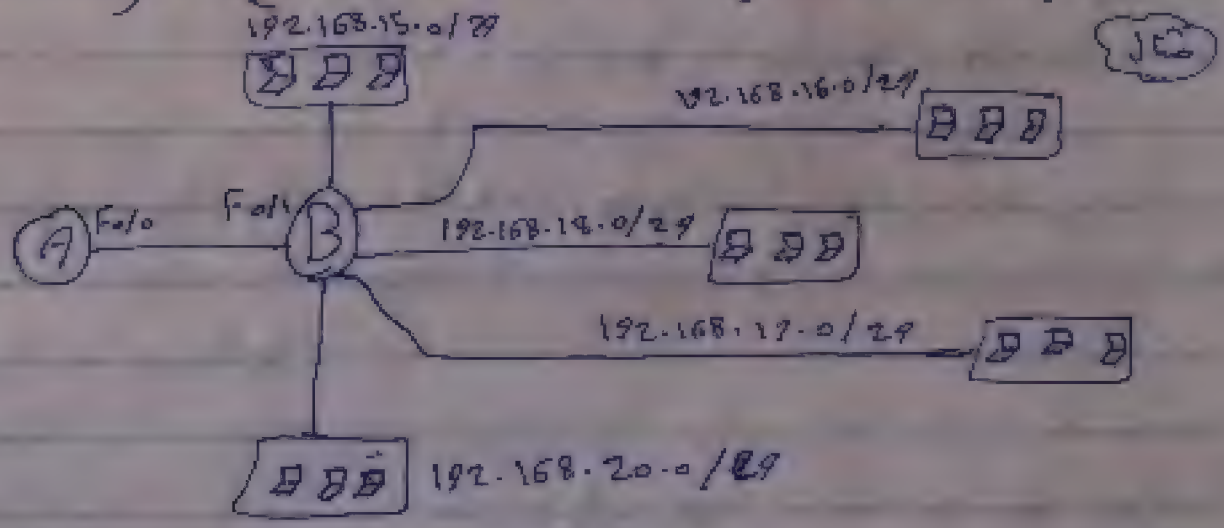
# Administrative distance AD

يستخدم الراوتر في المفاضلة بين الخطة الراوتنج بين الخطة  
 طبقاً لمعيارها Static وأيضاً Dynamic يستخدم الراوتر الـ AD  
 لإختيار ما هو أفضل الخطة التي ستخدمه ولذلك أيضاً لو كان Dynamic مرة  
 ospf ومرة Eigrp أو أن يكون أكثر من مرة يكون الـ Dynamic Route  
 فيستخدم الراوتر الـ AD ويختار أقل رقم

Route Type	Admin Distance
Connected	0
Static	1
Eigrp	90
ospf	110

## Summarization

الـ Supernetting أو ما يعرف بـ Summarization هو عملية تجميع  
 الشبكات إلى شبكة الأصل CIDR وهي عكس عملية الـ Subnetting



لاحظ وجود 5 شبكات مع Class C متصلة برouter B هذه الشبكات Connected  
 على الراوتر تكون بالنسبة للراوتر A إذا أردنا تفعيل الراوتنج Static فإنتا تقوم بتفعيل  
 الشبكات شبكة للراوتر حتى يتم ادراجهم في الـ Routing Table فكرة  
 الـ Summarization هي اختصار كل الشبكات مكتوبة الشبكة الأم التي تجمعهم



وإذا كان لا نستطيع أن نستعمل تقنيات المراسلة في هذه الحالة فنحن نستخدم التقنيات التالية  
كل بقعة بلاستيكية في تلك المنطقة من تقويم Summer يجب أن تكون  
تقوم برفع البطاقات تحتها

192 168 15.0

192 168 14.0

192 168 17.0

192 168 18.0

192 168 21.0

هذا هو مجموع البطاقات هو 29.0 في هذه الحالة. البطاقات التي تكون في هذه الحالة  
في سيجو ماتش [192-168] هي الخلفاء المراسلة التي تكون تحتها  
في المراسلة و البطاقات في الخلفاء هي المراسلة

15.0 00000000

16.0 00000000

17.0 00000000

18.0 00000000

19.0 00000000

000 000000

تكون بطاقات في المراسلة هي المراسلة في المراسلة في المراسلة

في المراسلة هو [192 168 0.0] و المراسلة هو 16

في المراسلة هو [192 168 0.0/19] و المراسلة هو Summerized هو

شأنهم في المراسلة هو 207.21 و المراسلة هو 16.4/21 و المراسلة هو 207.21  
في المراسلة هو 207.21 و المراسلة هو 207.21

207.21 00000000

207.21 00000000

207.21 00000000

شأن آخر الشبكة 200.179.98.32/28 { 200.179.98.64/27 { 200.179.98.96/27 { 200.179.98.128/27  
 فعل هو Summarization التالي

الجزء الثابت هو 200.179.98  
 فإنه ل Binary

$$\begin{array}{rcl} 32 & = & 00100000 \\ 64 & = & 01000000 \\ 96 & = & 01100000 \end{array}$$

0000000

في الوقت الرابع هو صف ولكنه الخاطئ بين عدد الفعاليات  
 الثالث وهو ① حيث أنه عدد البتات الثابت في الوقت للثالث أي 24 هو الثابت  
 الأول فقط في ال cidr هو 200.179.98.0/25

شأن آخر الشبكات 200.179.98.0/25 { 200.179.99.0/25 { 200.179.56.0/23  
 فعل هو Summarization التالي

ال output الثابت هو 200.179 وار output المختلف هو الثالث  
 فإنه ل Binary

$$\begin{array}{rcl} 98 & = & 00110000 \\ 99 & = & 00110001 \\ 56 & = & 00111001 \end{array}$$

00110000

بالتالي العنوان هو 200.179.98.0 والـ 20 هو  
 فيكونه ال cidr هو 200.179.98.0/20



# ACL

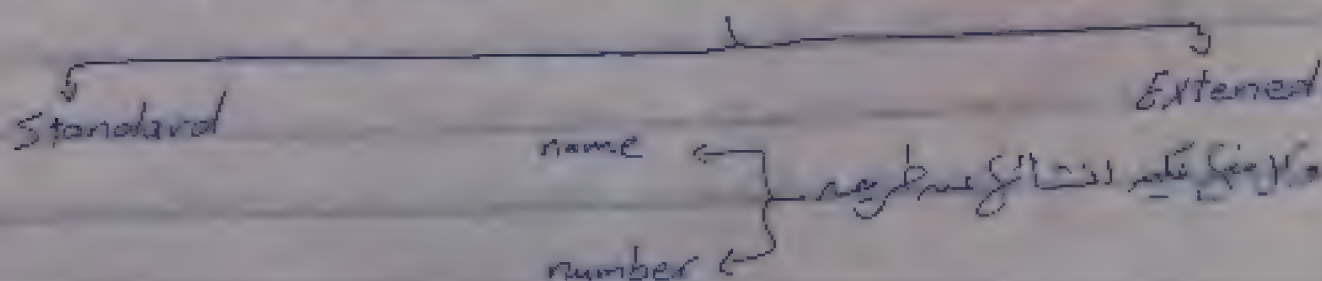
## Access Control List

هي مجموعة القوائم يتم تطبيقها على الواجهة التي من أساسها الممنوعة أو المسموحة  
معظم البيانات الغير مرغوب بها يتم السماح بالبيانات الممنوعة على أنه بالاحتفاظ بالبيانات  
من غير ذلك الممنوع أو الممنوع يتم تطبيقها على الشبكة فمنها القوائم التي تمنع الشبكة  
فإنه من منع شبكة بالخطوط الممنوعة من حيث السماح للجهاز أو أحد هذه الشبكة أن يتصل  
الاستراتيجية

تصانيفها

- (1) هي عبارة عن مجموعة من القوائم التي يتم تطبيقها على الشبكة  
(2) هذه الجمل يتم تطبيقها بطريقة تسلسلية مرتبة مثال ذلك لو أردنا  
أن تمنع الجهاز (أ) من الاتصال بالإنترنت وهذا الجهاز ضمن الشبكة رقم (10) فإنه الأمر هو  
منع الجهاز رقم (10) السماح للشبكة (10) وبالتالي الأمر رقم (10) هو منع الجهاز (10)  
والسماح للجهاز (10) فكله إذا كتبنا السماح للشبكة (10) أي أن الأمر رقم (10) هو السماح  
بمنع الجهاز رقم (10) هناك جهاز يمنع الجهاز (10) فكله إذا كتبنا منع (10) فكله هناك  
أمر بالسماح (10) بالرد على الإنترنت وبالتالي التسلسل والترتيب أمر مهم
- (3) الأمر رقم (10) هو منع الجهاز (10) هناك أمر رقم (10) لا يمنع ولا يسمح فكله يتم تطبيقه  
بجهد انتار قائمة ACL يعني أن إذا منعت الجهاز (10) مثلاً وحاول  
الجهاز (10) الاتصال بالإنترنت فإنه لن يستطيع بالرقم (10) هو السماح للجهاز (10) بالرد على الإنترنت  
لأنه هناك أمر رقم (10) هو منع الجهاز (10) فكله إذا كتبنا منع (10) فكله هناك  
فمنع السماح للجهاز (10) بالرد على الإنترنت
- (4) الـ ACL تنقسم إلى Global mode ويتم تطبيقها على الواجهة  
المراد تطبيقها على الواجهة

## # أنواع الـ Access List



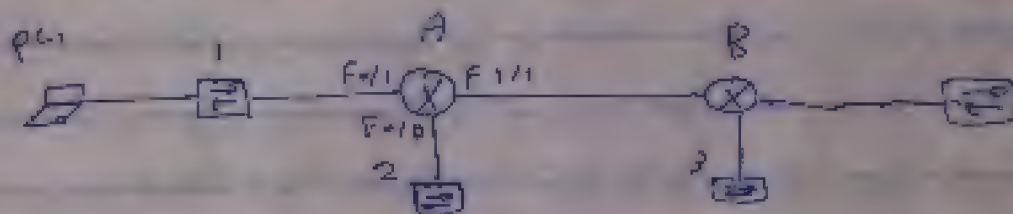
# Standard Acls

هذه هي الطريقة التي يتم فيها كتابة ACLs وتستخدمها Standard Acls  
 Name (P) الطريقة أو Name  
 Router (config) # ip Access-list standard < name > < source ip > < wildcard > < action >

1- إنشاء قائمة الوصول سوار deny أو permit  
 Router (config - std-nacl) # deny 192.168.10.1 + wildcard  
 Router (config - std-nacl) # permit any

2- تطبيقها على الواجهة

لا بد أن يتم تطبيقها على الواجهة Accesslist وبالنسبة إلى Accesslist في اتجاه in أو out للراوتر. وهذا يستلزم أن نحدد اتجاه Accesslist



نرى من هذه الشبكات أن كل الشبكات المتصلة بها  
 مسار البيانات من المصدر إلى الوجهة عبر الواجهة F0/1 و بالتالي نطبقها  
 على R1 على اتجاه in لأننا نريد منع البيانات من الوصول إلى R1 من  
 PC1. هذا هو السبب في أن اتجاه Accesslist هو in أو out.  
 في المثال لو أردنا أن نمنع البيانات من الوصول إلى R1 من  
 PC1 عبر الواجهة F0/10، فإننا نطبقها على R1 على اتجاه out لأننا  
 نريد منع البيانات من الخروج من R1 عبر الواجهة F0/10 إلى PC1.  
 وبالتالي نطبقها على R1 على اتجاه out لأننا نريد منع البيانات من الخروج من R1 عبر الواجهة F0/10 إلى PC1.  
 وبالتالي نطبقها على R1 على اتجاه out لأننا نريد منع البيانات من الخروج من R1 عبر الواجهة F0/10 إلى PC1.  
 وبالتالي نطبقها على R1 على اتجاه out لأننا نريد منع البيانات من الخروج من R1 عبر الواجهة F0/10 إلى PC1.



ممكن ان يكون

Router(config-if) # ip Access-group الاسم الرقم  
الاسم : اسم المجموعة  
الرقم : رقم المجموعة

ممكن ان يكون الاسم هو:

Router(config) # ip Access-list standard < name >

Router(config) # permit host \_\_\_\_\_

Router(config-std-nacl) # deny \_\_\_\_\_ <sup>IP</sup> + wild card (خريطة)

Router(config-std-nacl) # permit any

Router(config-std-nacl) # exit

Router(config) # int Fast 0/1

Router(config-if) # ip Access-group الاسم +  $\frac{out}{in}$  or

ملاحظة: في named Acls (الرقم) من (1 : 99) هو ارقام standard

في التالى لو اردنا ان نعمل تغيير فى امر ما. تتبع الاتى

1) امر الاسم show لعرض رقم الامر

Show Access-list

سيظهر بعض الاجراءات التى تم تنفيذها وقيل امر ال permit هو 20 و امر

ال deny كان 50 فلو كانت محتاج اضافة امر بينهم الى امر الارقام السابقة

بعض طريقة الامر show

© كتابة الامر الجديد بعد اضافة الرقم المناسب عن طريق الامر

Router(config) # ip Access-list standard (الاسم السابق)

Router(config-std-nacl) #  $\frac{permit}{deny}$  + رقم

ونحدد الرقم حسب المراتب التى عليه لو اردنا ان نضيف امر نكتب رقم بعد

الرقم امل الامر وهكذا

⑤ طريقة الترميز في ACL

أولاً حدد رقم الـ Access List (99 : 199) ثم حدد نوع الـ Access List (Standard Access List)

ثانياً اكتب الأرقام التي تريد السماح بها أو نفيها في الـ Named Access List

ثالثاً اكتب الـ Access List

Router(Config) # Access-list + رقم +  $\frac{\text{deny}}{\text{permit}}$  + host + ip source

مثال

Router(Config) # Access-list + رقم +  $\frac{\text{deny}}{\text{permit}}$  + source ip + subnet mask ~~0.0.0.0~~

Router(Config) # Access-list + رقم + permit any

⑥ تفعيل الـ Access List على الواجهة

Router(Config-if) # ip Access-group + رقم +  $\frac{\text{in}}{\text{out}}$  or

مثال: لدينا واجهة 18.0.2.3/23 نريد السماح بها

Router(Config) # Access-list + رقم + permit + ip source + subnet mask

هنا نريد السماح بها إذا كان الـ IP الـ Source

فإننا نكتب الـ wildcard mask 0.0.0.0

Standard Config

① السماح بها

Router(Config) # Access-list + رقم +  $\frac{\text{permit}}{\text{deny}}$  + host + ip source 0.0.0.0

Router(Config) # Access-list + رقم +  $\frac{\text{permit}}{\text{deny}}$  + ip source + subnet mask

② نفيها

Router(Config) # Access-list + رقم +  $\frac{\text{deny}}{\text{permit}}$  + ip source + wildcard mask

⑦ تفعيل الـ Access List على الواجهة

Router(Config-if) # ip Access-group + رقم +  $\frac{\text{in}}{\text{out}}$

Router # Show Access-list



## Extended Access List (2)

هذا النوع من الترخيص يقيّم ثبات packet العنصرين الأخيرين Source IP و Destination IP وذلك نوع البروتوكول وكذلك رقم البورت وبالتالي هذا النوع يتيح لنا التحكم في القلم من الشبكة أكثر من النوع Standard

(P) طريقة ال Name

Router(Config) # ip Access-list extended < >

Router(Config-ext-nacl) # permit < البروتوكول > host source host destination < >  
مثال

Router(Config-ext-nacl) # permit ~~ip~~ host 18.0.2.3 host 18.0.0.9 eq 69

Router(Config-ext-nacl) # deny ~~ip~~ host . . . . . مثال آخر

Router(Config-ext-nacl) # permit icmp any any

\* تعطى لكل البورت بعد تسمية ال in أو out على الراوتر

Router(Config-if) # ip access-group < > in / out

(3) طريقة ال number

ال extended ال، مثل الخاصة بـ 199 : 1000  
أو 1000 : 999

Router(Config) # Access-list 110 deny TCP host IP + host IP eq البروتوكول

Router(Config) # Access-list 110 permit TCP any any

\* التفعيل على البورت

Router(Config-if) # ip Access-group in

و الصفحة التالية فيجئ ال Configuration الخاصة بـ Access-list  
بصورة أوسع

① منع IP من host

Router(Config) # Access-list 101 deny ip host IP host IP

Router(Config) # Access-list 101 permit ip any any

② منع IP من host مع network و wildcard

Router(Config) # Access-list 102 deny ip host IP + network + wildcard

Router(Config) # Access-list 102 permit IP any any

③ منع IP من host مع network و wildcard

Router(Config) # Access-list 103 deny IP network + wildcard + network + wildcard

Router(Config) # Access-list 103 permit any any.

④ منع IP من host مع network و wildcard و host و IP

Router(Config) # Access-list 104 deny ~~host~~ ip network + wildcard + host IP

Router(Config) # Access-list 104 permit ip any any

⑤ إعدادات ال Telnet

1- أملاك فقط خاصية ال Remote Access بالطريقة العادية

2- تكتب ال إعدادات ال global mode

Router(Config) # Access List + رقم +  $\frac{\text{deny}}{\text{permit}}$  + host IP source

أو

Router(Config) # Access-list + رقم +  $\frac{\text{deny}}{\text{permit}}$  + IP source + 0.0.0.0

⑥ طرق ال إعدادات ال VTY

Router(Config) # Line VTY 0 9

Router(Config-line) # Access-class +  $\frac{\text{in}}{\text{out}}$  +  $\frac{\text{deny}}{\text{permit}}$  + الرقم

Router(Config) # no Access-list + الرقم واللغز لغز



## أوامر show في الـ Access-list

- R# show access-list → يعرف كل الـ Access-list
- R# show access-list 110 → يعرف الـ Access-list برقمها 110
- R# show ip interfaces → يعرف كل حدة على الـ interface
- R# show running-config → يعرف كل حدة

هناك انقسام على الـ Named Access-list ولا يمكن القبول على numbered Access-list كلمة أخرى الـ Access-list هي فقط لتأجيل.

## DHCP

تواضعها Dynamic Host Configuration protocol ويعني بالعربية بروتوكول التهيئة الديناميكية وهو بروتوكول يقوم بإعداد نظامية (IP) لأجهزة الشبكة بصورة أوتوماتيكية بدلاً من الطريقة اليدوية.

### س: كيف يعمل DHCP ؟

هناك 4 خطوات لكي يعمل أي جهاز على عنوانه من خلال DHCP

1. Dhcp discover

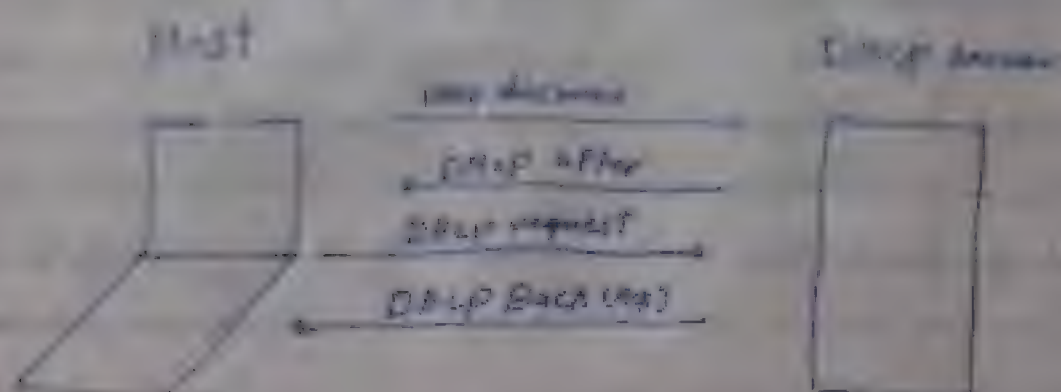
يقوم الـ Host في هذه الخطوة بإرسال رسالة على شكل Broadcast فيرسلها إلى 255.255.255.255 في صيغة أنه هذا لا يملك عنوانه فيكون عنوانه في هذه الخطوة هو 0.0.0.0 أما 0.0.0.0 يرسل إلى 255.255.255.255 رسالة تنقسم الـ mac address

### 2. Dhcp offer

عندما تصل رسالة الـ Host للعنوان 255.255.255.255 فإنها تصل لكل الأجهزة في الشبكة ومنه فمنها سيرسل الـ DHCP الذي يريد عليه يعرف خدماته من خلال Dhcp offer وينبغي يقرر على الجهاز الطالب عنوان IP مع باقي المعلومات المسماة به ويتم حجز هذا العنوان بشكل مؤقت لحين ورود تأكيد يقوله من الجهاز الـ Host

3. Dhcp request → يقوم الـ Host بالرد على سيرفر بإرسال Dhcp request تأكيد بتلقيه استخدام العنوان المقترح

في DHCP Server  
 مخصص لها IP address pool من بين بروتوكول السيرفر في DHCP server  
 مخصص



المسألة من اعداد سيرفر DHCP مياتنا نقوم بالآتي:

\* تحديد مجال [ بناءً على ] العنصر الذي سيتم تخصيصه للأجهزة و Default mask

\* تحديد العنصر الذي سيتم تخصيصه له من بين العنصر الذي هو العنصر الذي سيتم تخصيصه له

الأجهزة التالية التي لا مجال لتغييرها أو تغييرها بالسيرفرات

\* تحديد العنصر الذي سيتم تخصيصه له من بين العنصر الذي هو العنصر الذي سيتم تخصيصه له

\* عنوان ال Default gateway

\* عنوان سيرفر ال DNS

## # DHCP Configuration #

① اختيار DHCP address pool وإعطائه اسم

Router(config) # ip dhcp pool name

② تحديد العنصر الذي سيتم تخصيصه له من بين العنصر الذي هو العنصر الذي سيتم تخصيصه له

Router(dhcp-config) # network network + mask

③ تحديد ال Default gateway

Router(dhcp-config) # default-router + IP gateway

④ تحديد ال DNS

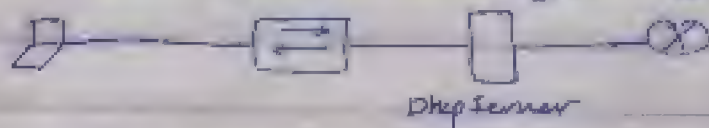
Router(dhcp-config) # dns-server IP



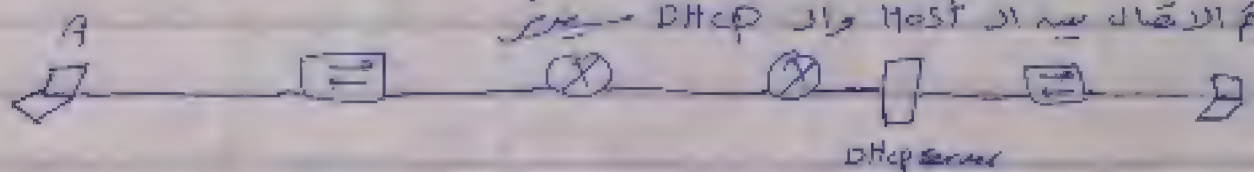
(5) ملاحظة: عند إعداد الـ DHCP  
 Router(Config) # ip dhcp excluded address 19 20  
 (من 19 إلى 20)

(6) تحديد وقت الـ lease في الـ DHCP  
 Router(Config) # lease 1 5 20 30  
 ساعة دقيقة ثانية

• لو السيرفر DHCP من شبكة أخرى  
 ابتداءً عننا نقوم الـ Host بإرسال رسالة الـ Discover فالتالي الـ Offer  
 على هيئة Broadcast فتقبل كل الأجهزة المتصلة في نفس الشبكة.



فكرة: إذا كان السيرفر من شبكة ثانية تفعل بينه وبين أجهزة الراوتر خيار رسالة الـ Broadcast لأن رسالة الراوتر لا تخرج من الشبكة التي هي فقط وبالتالي لن يتم الاتصال بين الـ Host والـ DHCP سيرفر.



ولكن قبل هذه العملية نفعل أمر يتيح لنا الحصول على DHCP سيرفر من نفس الشبكة  
 جديدة وهو الأمر helper address Ip ولكن نرسل أنه الـ gateway تكون الشبكة المراد الحصول  
 على DHCP سيرفر من. ويكون الأمر كالآتي:

① تمديد الأمر في الـ Host

Router(Config) # int 0/0/0 مثال

② تمديد الأمر Helper address

Router(Config-if) # ip helper address dhcp server

# أمر الـ show الخاص بـ DHCP  
 show ip dhcp pool . show ip dhcp binding . show ip dhcp conflict  
 clear ip dhcp conflict.

ويمكن معرفة الـ IP الذي حصل عليه الجهاز بطريقة أمر الـ Run

ipConfig /all

# NAT

هو اختصار Network address Translation وتعمل الآلة على التحويل بين نوعي العناوين الخاصة بـ private addressing والـ Real Ips

## ① Private addressing

تتم مجموعة من العناوين التي تم حجزها للاستخدامات الخاصة داخل الشبكات المحلية للمنظمات أو في الشبكات البيئية وهي خاصة لأنها لا يمكن أن تكون جهازاً أو سيرفر أو مكتوباً مباشرة على حزمة الإنترنت يعمل واحداً من هذه العناوين فهي غير مرتبطة بأي نظام domain على الإنترنت

## ② هذه العناوين الخاصة بـ private تظهر في الجدول التالي

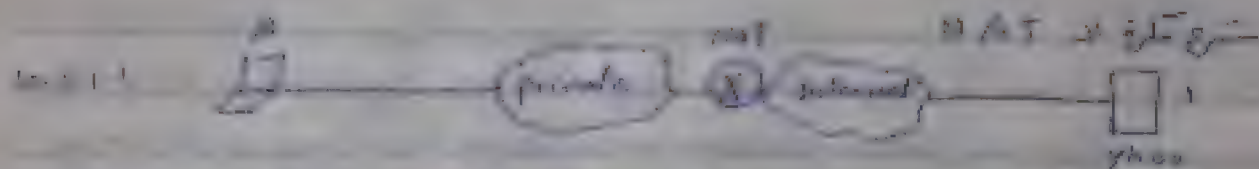
Range of IP addresses	Class	Number of networks
10.0.0.0 To 10.255.255.255	A	1
172.16.0.0 To 172.31.255.255	B	16
192.168.0.0 To 192.168.255.255	C	256

③ الـ Real Ips هي العناوين التي يمكن الاتصال مباشرة بالإنترنت  
دونه الحاجة لوسيط

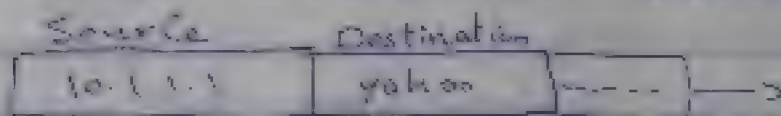
## فكرة عمل الـ NAT

هو عملية تحويل الـ private ip من الوصول على الإنترنت بطريقة تحويل الـ private ip إلى الـ real ip عند محاولة الوصول إلى الإنترنت حيث أنه الوصول إلى الـ Real ip يتطلب ملفاً جديداً . وبذلك تحول الـ private ip واحد إلى أكثر من الـ real ip واحد أو أكثر من واحد





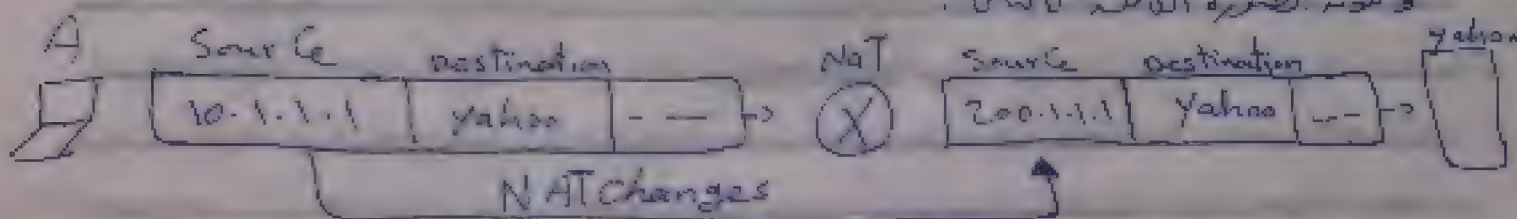
مفهومنا هو عندما نريد الوصول إلى موقع معين مثل yahoo فإننا نستخدم عنواننا الخاص (private IP) عندما نقل البيانات نقوم بتغييره



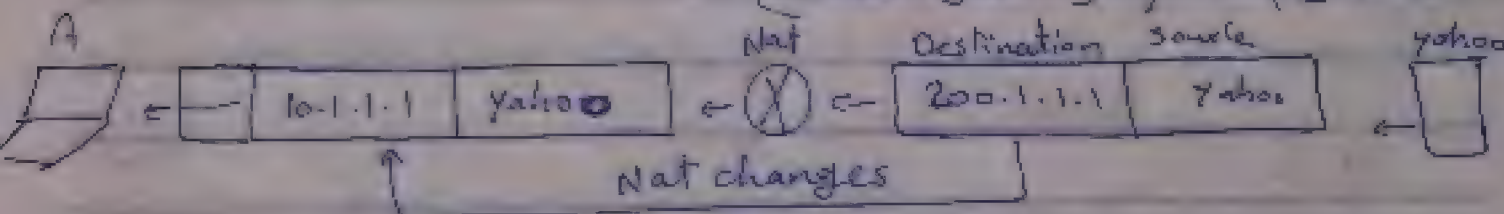
وعندما نقل البيانات نقوم بتغييره إلى Nat غير سواء ال Source ووجهة ال Destination  
الوجهة ال Destination إلى real IP فيكون كالتالي



وتكون الصورة التالية كالتالي

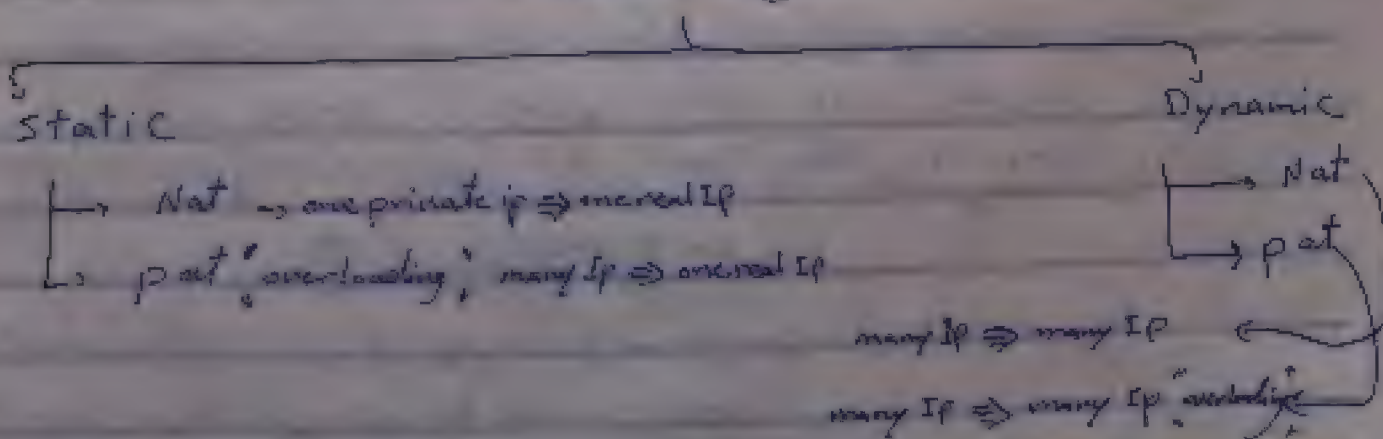


وعندما نقوم بالرد نقول العكس



هذه الطريقة هي التي يتم استخدامها كإنترنت IP خاصة بالهاتف المحمول

## أنواع الـ NAT



PAT = port address translation

— *Estadística* *1997* □

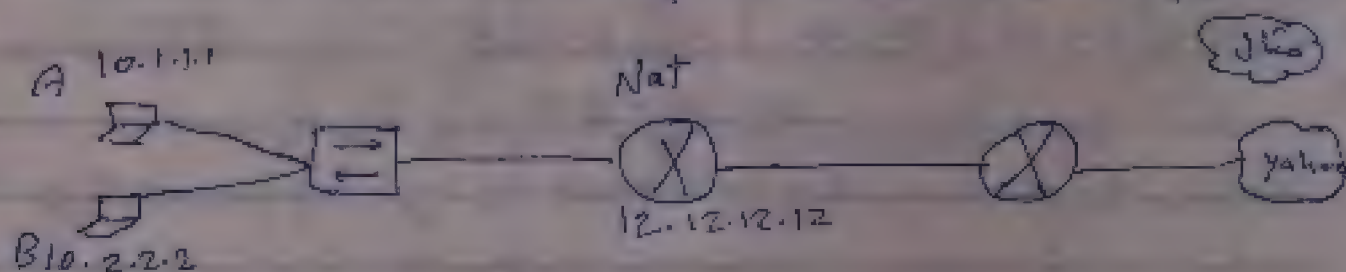
تفاتيح القبول:  $pk = (N, e)$  حيث  $N = p \cdot q$  و  $e$  هي دالة التشفير.  
 المفاتيح الخاصة:  $sk = (p, q, d)$  حيث  $d$  هي دالة فك التشفير.

Определенный интеграл

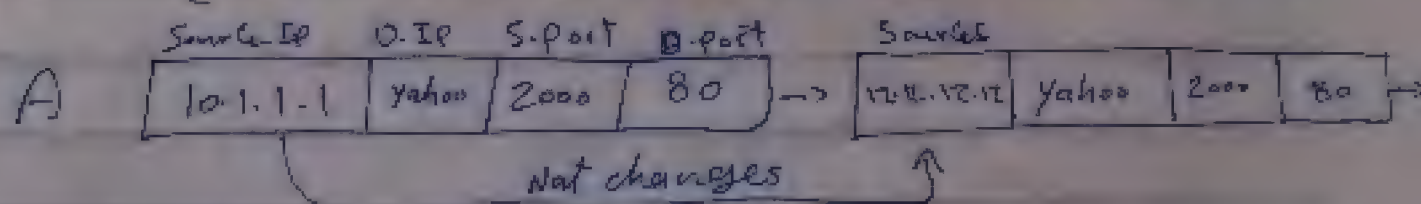
هنا يتم التحويل بين مجموعة من المتغيرات الخاصة بمجموعة أخرى باسم المتغيرات  $z$  ويتم اختيار ال  $z$  الذي سيخرج منتج ال  $private$  بشكل عشوائي أي  $z$  من مجموعة ال  $z$  المتاحات في  $z$  ولأنه عند  $z$  فاص يخرجون كل  $z$  له  $z$  له  $z$  ينتج الباقي  $z$  ينتج  $z$  الخاصة ليخرج واحد فكله لا يخرج.

→ pot 7

هذا اختصار port address translation أو ما يُعرف بالترجمة الدينامية Dynamic وهو الأكثر شيوعاً. ففي جميع الأجهزة تتقدم بفتح عنوان الذاكرة address وكذلك يتم التمييز بين أساس رقم متقدم المرسل للتمييز بين كل متقدم من التبلية الداخلية وفي حال كان جهازاً به يتقدمون بفتح المتقدم بفتح الراوتر فيغير أحد المتقدمين ويكمل هذه العملية مع بروتوكول Tcp و Udp فقط ولكن يوجد نظام لـ Icmp



بفرقة أنه الجهاز A يرسل إلى  $MSK_{\text{mod}}$  في شكل النبضة يكون به الخندق الذي خرج منه  
أما أن يتخذ الجهاز A ويحوي أيضاً على النبوة الخاصة بالضغط

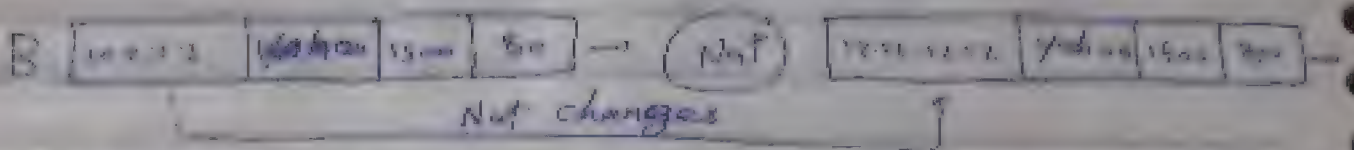


نقد و نظر آنکه اینک است اقوت این رقم منفذ کل به المرسد میگوید رقم بعد ۱۰۴۹ و رقم منفذ العالی اما المستقبل وهو ۸۵ الخاص بالصفحة.

المادة 10: تم تقديم البعثة والتمثيل الجهازي B في طيغ استقام



تحت الـ real IP يتم تغير المنفذ التالي



نلاحظ أنه الجهاز B (10.2.2.2) استخدم قسماً الـ 50 من الـ real IP  
[12.34.56.7] ورقته استخدم بورت آخر غير بورت الجهاز A وهو (1500) من حصة  
أه الجهاز B استخدم (2000)

من حالة أن الجهازية استخدم نفس المنفذ واضطرر المنفذ (2000) متارياً  
المراتب يجب أن يصحح أنه هذا المنفذ محجوز وبالتالي عليك استخدام غيره

ملاحظة اختيار الجهاز المنفذ الذي تخصصه يتم بشكل عشوائي لذلك قد تحدث  
الاستقرار في المنفذ الذي يجب عليه المراد تركا في الخطوة السابقة

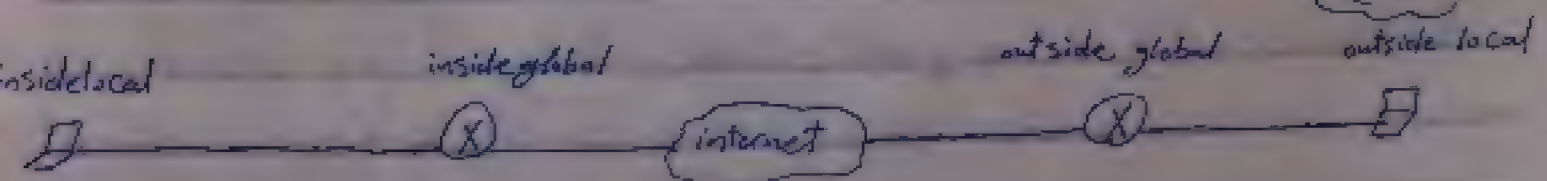
تتميز هنا طريقة static NAT أما استخدام real IP واحدة لكل الأجهزة ورقته  
من الـ Dynamic NAT أقل حيث لا يميز ضغط كبير على الـ real IP

من الـ PAT نفس أيضاً overloading حيث يتم تحميل عدد كبير من الـ real IP  
في الـ private IP.

## ملاحظات هامة

- ① Inside local ← الجهاز الداخلي من شبكتي الذي يكون عنوانه خاص private
- ② Inside global ← الجهاز الداخلي في الراوتر الذي يمتلكه الذي يكون عنوانه real
- ③ Outside global ← الجهاز الخارجي في الراوتر الثاني الذي يكون عنوانه real
- ④ Outside local ← الجهاز الخارجي في الشبكة الأخرى الذي يكون عنوانه private

الشرح



## NAT configuration

### static NAT [1]

Static NAT ١ مثال

Router(config) # ip nat inside source static + private ip + real ip

تعريف الانترنت الداخلي

Router (config-if) # ip nat inside

٢ تعريف الانترنت الخارجي "الانترنت" لتعرفت

Router (config-if) # ip nat outside

### Dynamic NAT [2]

١ قم بال Nat pool وتسمية واتخذ ال range الخاص به وتلك ال IP وانها ال range

Router(config) # ip nat pool + اسم + first ip from the range + end of range + netmask

Router(config) # ip nat inside source list 50 + pool + اسم pool

٢ اسم Access list لتعريف ال real ip

Router(config) # Access-list 50 permit + عنوان الشبكة + wild mask

٣ تعريف الانترنت الداخلي

Router (config-if) # ip nat inside

٤ تعريف الانترنت الخارجي

Router (config-if) # ip nat outside

### PAT [3]



PAS

2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2031, 2032, 2033, 2034, 2035, 2036, 2037, 2038, 2039, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2059, 2060, 2061, 2062, 2063, 2064, 2065, 2066, 2067, 2068, 2069, 2070, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078, 2079, 2080, 2081, 2082, 2083, 2084, 2085, 2086, 2087, 2088, 2089, 2090, 2091, 2092, 2093, 2094, 2095, 2096, 2097, 2098, 2099, 2100, 2101, 2102, 2103, 2104, 2105, 2106, 2107, 2108, 2109, 2110, 2111, 2112, 2113, 2114, 2115, 2116, 2117, 2118, 2119, 2120, 2121, 2122, 2123, 2124, 2125, 2126, 2127, 2128, 2129, 2130, 2131, 2132, 2133, 2134, 2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2144, 2145, 2146, 2147, 2148, 2149, 2150, 2151, 2152, 2153, 2154, 2155, 2156, 2157, 2158, 2159, 2160, 2161, 2162, 2163, 2164, 2165, 2166, 2167, 2168, 2169, 2170, 2171, 2172, 2173, 2174, 2175, 2176, 2177, 2178, 2179, 2180, 2181, 2182, 2183, 2184, 2185, 2186, 2187, 2188, 2189, 2190, 2191, 2192, 2193, 2194, 2195, 2196, 2197, 2198, 2199, 2200, 2201, 2202, 2203, 2204, 2205, 2206, 2207, 2208, 2209, 2210, 2211, 2212, 2213, 2214, 2215, 2216, 2217, 2218, 2219, 2220, 2221, 2222, 2223, 2224, 2225, 2226, 2227, 2228, 2229, 2230, 2231, 2232, 2233, 2234, 2235, 2236, 2237, 2238, 2239, 2240, 2241, 2242, 2243, 2244, 2245, 2246, 2247, 2248, 2249, 2250, 2251, 2252, 2253, 2254, 2255, 2256, 2257, 2258, 2259, 2260, 2261, 2262, 2263, 2264, 2265, 2266, 2267, 2268, 2269, 2270, 2271, 2272, 2273, 2274, 2275, 2276, 2277, 2278, 2279, 2280, 2281, 2282, 2283, 2284, 2285, 2286, 2287, 2288, 2289, 2290, 2291, 2292, 2293, 2294, 2295, 2296, 2297, 2298, 2299, 2300, 2301, 2302, 2303, 2304, 2305, 2306, 2307, 2308, 2309, 2310, 2311, 2312, 2313, 2314, 2315, 2316, 2317, 2318, 2319, 2320, 2321, 2322, 2323, 2324, 2325, 2326, 2327, 2328, 2329, 2330, 2331, 2332, 2333, 2334, 2335, 2336, 2337, 2338, 2339, 2340, 2341, 2342, 2343, 2344, 2345, 2346, 2347, 2348, 2349, 2350, 2351, 2352, 2353, 2354, 2355, 2356, 2357, 2358, 2359, 2360, 2361, 2362, 2363, 2364, 2365, 2366, 2367, 2368, 2369, 2370, 2371, 2372, 2373, 2374, 2375, 2376, 2377, 2378, 2379, 2380, 2381, 2382, 2383, 2384, 2385, 2386, 2387, 2388, 2389, 2390, 2391, 2392, 2393, 2394, 2395, 2396, 2397, 2398, 2399, 2400, 2401, 2402, 2403, 2404, 2405, 2406, 2407, 2408, 2409, 2410, 2411, 2412, 2413, 2414, 2415, 2416, 2417, 2418, 2419, 2420, 2421, 2422, 2423, 2424, 2425, 2426, 2427, 2428, 2429, 2430, 2431, 2432, 2433, 2434, 2435, 2436, 2437, 2438, 2439, 2440, 2441, 2442, 2443, 2444, 2445, 2446, 2447, 2448, 2449, 2450, 2451, 2452, 2453, 2454, 2455, 2456, 2457, 2458, 2459, 2460, 2461, 2462, 2463, 2464, 2465, 2466, 2467, 2468, 2469, 2470, 2471, 2472, 2473, 2474, 2475, 2476, 2477, 2478, 2479, 2480, 2481, 2482, 2483, 2484, 2485, 2486, 2487, 2488, 2489, 2490, 2491, 2492, 2493, 2494, 2495, 2496, 2497, 2498, 2499, 2500, 2501, 2502, 2503, 2504, 2505, 2506, 2507, 2508, 2509, 2510, 2511, 2512, 2513, 2514, 2515, 2516, 2517, 2518, 2519, 2520, 2521, 2522, 2523, 2524, 2525, 2526, 2527, 2528, 2529, 2530, 2531, 2532, 2533, 2534, 2535, 2536, 2537, 2538, 2539, 2540, 2541, 2542, 2543, 2544, 2545, 2546, 2547, 2548, 2549, 2550, 2551, 2552, 2553, 2554, 2555, 2556, 2557, 2558, 2559, 2560, 2561, 2562, 2563, 2564, 2565, 2566, 2567, 2568, 2569, 2570, 2571, 2572, 2573, 2574, 2575, 2576, 2577, 2578, 2579, 2580, 2581, 2582, 2583, 2584, 2585, 2586, 2587, 2588, 2589, 2590, 2591, 2592, 2593, 2594, 2595, 2596, 2597, 2598, 2599, 2600, 2601, 2602, 2603, 2604, 2605, 2606, 2607, 2608, 2609, 2610, 2611, 2612, 2613, 2614, 2615, 2616, 2617, 2618, 2619, 2620, 2621, 2622, 2623, 2624, 2625, 2626, 2627, 2628, 2629, 2630, 2631, 2632, 2633, 2634, 2635, 2636, 2637, 2638, 2639, 2640, 2641, 2642, 2643, 2644, 2645, 2646, 2647, 2648, 2649, 2650, 2651, 2652, 2653, 2654, 2655, 2656, 2657, 2658, 2659, 2660, 2661, 2662, 2663, 2664, 2665, 2666, 2667, 2668, 2669, 2670, 2671, 2672, 2673, 2674, 2675, 2676, 2677, 2678, 2679, 2680, 2681, 26

[illegible]

Dynamic  $pA^+$  @

② انتصار ال Pool وفتح ال Range وفتح ال Pool

$$\text{Number}(\text{Config}) \neq \text{if stat } p=0 \rightarrow p=0, p=1 \rightarrow \text{range in } [p, 1] + \text{range in } [1, 1] + \text{not in stat}$$

Access: ٢٠١٦-١١-١٥

Router (Config) # ip Access-List standard Almost 3K

`docker (config-stol-nsl) # permit + allow + wildcard`

④ تحميل الملف من [https://www.accessdata.fda.gov/drugsatfda\\_docs/nda/2015/014109Orig1s001.pdf](https://www.accessdata.fda.gov/drugsatfda_docs/nda/2015/014109Orig1s001.pdf) ونسخة كلمة download

Router(config) # ip nat inside source list Ahmed pool1 + pool2 ~ 1 + overload

(4) تكمية الانتزاع من المعاجلة

(config-if) # ip nat inside.

⑤ تحديد الانتماء إلى الفصيلة

(config-if) ~~un~~ ip nat outside.

Show that

### # Show if Not Translation

# show ip nat static

clear

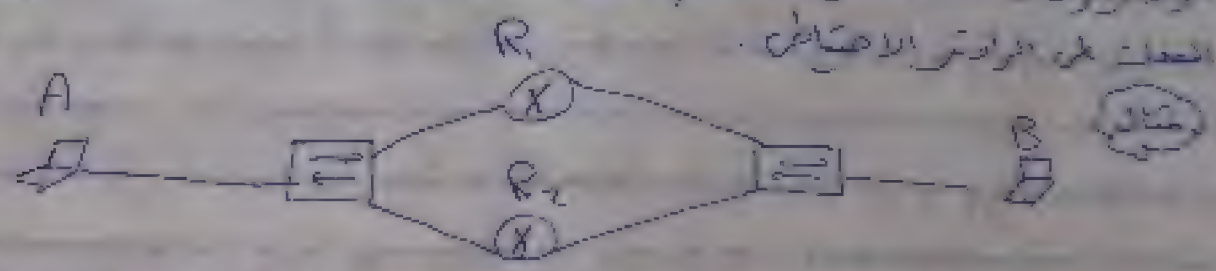
```
# clear Ip Net Translation.
```

\* امر Debug

```
-# debugging not
```

# First Hop Redundancy Protocol FHRP

يقوم هذا البروتوكول على توفير مسار بديل من حالة حدوث مشكلة في المسار الرئيسي من خلال عدة طرق. الراوتر احتياطي للراوتر الرئيسي ويتبع ذلك عدة طرق حيث أن بروتوكول بديل على الراوتر الرئيسي وذلك للراوتر الاحتياطي بحيث لو حدثت مشكلة في الراوتر الرئيسي فلا داعي للقلق إلى بروتوكول الشبكة لتقوم الشبكة إلى بروتوكول الصيانة على الراوتر الاحتياطي.



بفرض الجهاز A يريد أن يتصل بالجهاز B وال بروتوكول له في البورت على الراوتر R1. فلو حدثت مشكلة في هذا الراوتر يفقد الجهاز A القدرة على الاتصال B حيث أن بروتوكول redundancy هو R1 ففكرة FHRP هي كيفية الاستفادة من الراوتر R2 عند طرجه. إن شاء بروتوكول وجميع على كل من الراوترين يتكلمون لهم إلى بروتوكول للجهاز A بحيث لو حدثت مشكلة في الراوتر R1 الراوتر الرئيسي يتكلمون هناك مسار أو راوتر احتياطي لتتطبع الشبكة استتمام إلى بروتوكول الخاص به وهذا بالطبع يتكلمون إلى بروتوكول الوصفة المفعل على الراوترين في المثال حيث لا يتطبع أنه نشأ أكثر من بروتوكول حقيقة الشبكة وبالتالي بجانبنا لا تار بروتوكول وجميع مشتركة بين الراوترين.

أصبح FHRP

- 1- يعتمد من قدرة الشبكة على العمل
- 2- لو حدثت مشكلة يتكلم على طريقة المسار الاحتياطي

• انتشار FHRP لدينا 3 أنواع من البروتوكولات

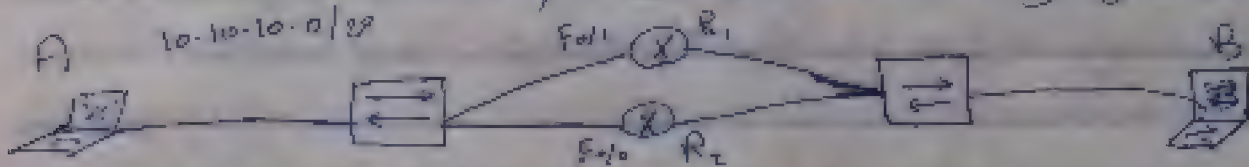
- ① HSRP
- ② VRRP
- ③ GLBP



# HSRP

HSRP هو اختصار لـ Hot Standby Router Protocol. وهو بروتوكول خاص يستخدم

لضمان استمرارية عمل الشبكة في حالة فشل الراوتر النشط. حيث يكون هناك راوتر نشط (Active) وآخر في حالة standby. في حالة فشل الراوتر النشط، يقوم الراوتر standby بالتأدية تلقائياً. هذه العملية تقوم بها أجهزة gateway. وتسمى هذه العملية بـ failover. وتكون الراوترات في حالة standby و Active. وكذلك ال standby



مثال: طرقتنا المتكاملة السابغ البهاز A يرسل حبات البهاز B وترميها في قفل HSRP على الراوترية مناهض الاعدادات التي تقوم بها ؟

## II اعدادات الراوتر R1

④ ندخل على الاشراف المواجه للتعطيل ونعطيه IP من ال شبكة

R1 (config) # int F0/1

R1 (config-if) # IP address 10.10.10.1 255.255.255.0

R1 (config-if) # No shutdown

⑤ نعمل standby لتقبل بروتوكول HSRP ونعطيه رقم ونضع ال gateway الواجهة

R1 (config-if) # standby 1 IP 10.10.10.5

نلاحظ اننا رقم العنصر هو (1) ويمكن اختيار غيره واضعنا ال gateway 10.10.10.5

⑥ تعديل ال priority لجعل هذا الراوتر هو الرئيس \* Active \*

Router (config-if) # standby 1 priority 150

نلاحظ اننا اسم العنصر (1) حتى نعمل على ال اساس وبالنسبة ال priority فاننا نضع ال اساس ال وضع الاشراف 100 وبالنسبة ال نضع ال الراوتر هو ال Active فزيده عن ال 100 وعليناها 150

(د) عقیقہ و شامیہ

فإنه قد انقسم من حيث هو إلى قسمين: قسم أول هو الذي لا يتغير مع تغير  
الزمان، والقسم الثاني هو الذي يتغير مع تغير الزمان. والقسم الأول هو الذي  
لا يتغير مع تغير الزمان، والقسم الثاني هو الذي يتغير مع تغير الزمان.

R. (config - if) # standby ! preempt

وقلت: أكون غلبت HSRP على الراوتر R<sub>1</sub> ويتوجب لتفعيل على R<sub>2</sub> Config

$$R_1(\text{config}) \neq \text{int } F_0/O$$

R2 (config-if) # ip address 10.10.10.2 255.255.255.0

R2 (config-if) # no shutdown

R2 (Config-if) # standby 1 IP 10.10.10.5 الواجهة الممركة

$R_2$  (config-if) #standby 1 preempt

وقبلنا فلو تم علينا HSRp واعمالنا في الامم الـ show

R. # Show standby brief

R. # Show standby

Virtual Router redundancy protocol.

VRRP (2)

هذا البروتوكول هو نفس فكرة بروتوكول HSRP لكنه VRRP يعمل على كل الأجهزة  
خلافاً HSRP فهو يعمل على أجهزة سيسكو فقط وبالنسبة للأجهزة من نفس  
أجهزة سيسكو تلك تستطيع أن تكون Master وتكون كذلك تستطيع standby  
تكون Backup أي يكون الرئيس هو الـ master والأجهزة هو الـ Backup





(أولتر رئيسي وهو صاحب أعلى Priority) ويملكها صاحب أعلى Ip أولتر في الواجهة  
 حوسبة الراوتر الرئيسي = AVF = Active Virtual Gateway ويقوم بتوزيع  
 بتوزيع الحمل في الواجهة على الواجهة. ومثال مرة سيطلب ARP لمالك أريد  
 يرسل مالك ويطلب من الخادم ثم يرسل الخادم إلى مالك يرسل مالك  
 الخادم الخادم به وبالتالي يتم إرسال الداتا عبر فلالة والـ ARP الثاني يرسل  
 مالك الخادم الراوتر الثاني فيتم إرسال الداتا عبر فلالة ومثلها وبالتالي تمت  
 عملية الـ load balance وهو أنه يتم توزيع الحمل على الواجهة وبالتالي الواجهة  
 الأخرى تسمى AVF = Active Virtual Forward

GIRP Config

```

Router(config) # int f0/0
Router(config-if) # ip address 10.10.10.1 255.255.255.0
Router(config-if) # no shutdown
Router(config-if) # glbp 3 ip 10.10.10.5
Router(config-if) # glbp 3 priority 110
Router(config-if) # glbp 3 preempt
    
```

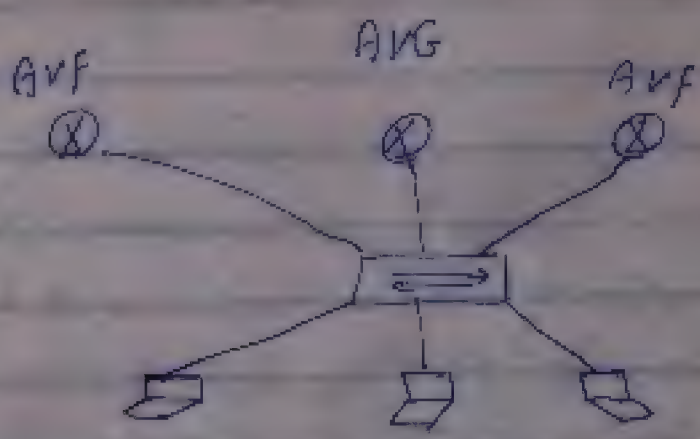
الـ priority = الأولوية المشتركة

متقبل ذلك على كل راوتر  
 أوامر show

```

Router # show glbp
Router # show glbp brief or group - interface
    
```

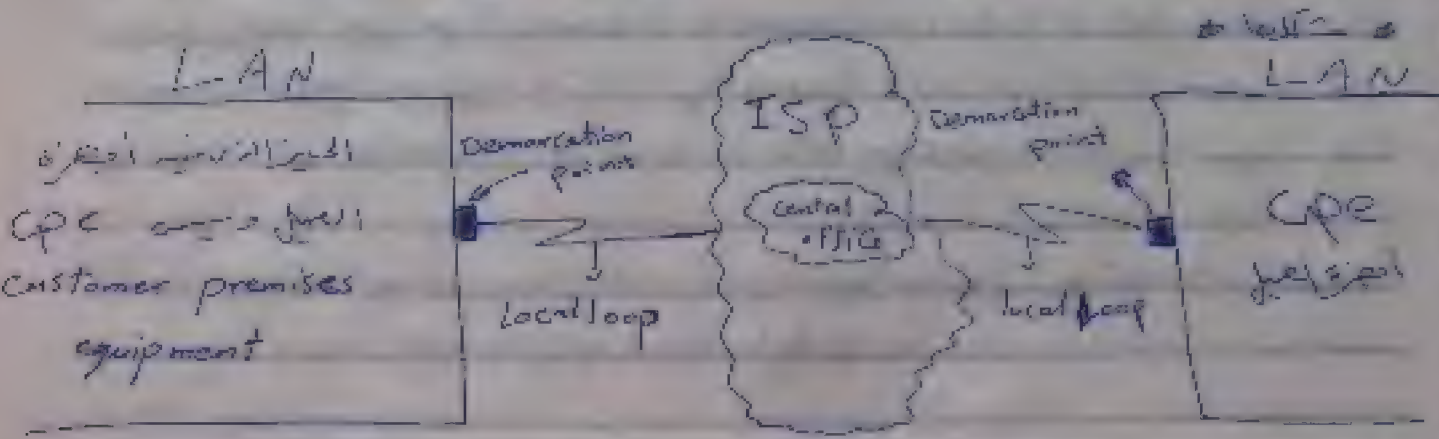
مكان تشكيل الـ glbp





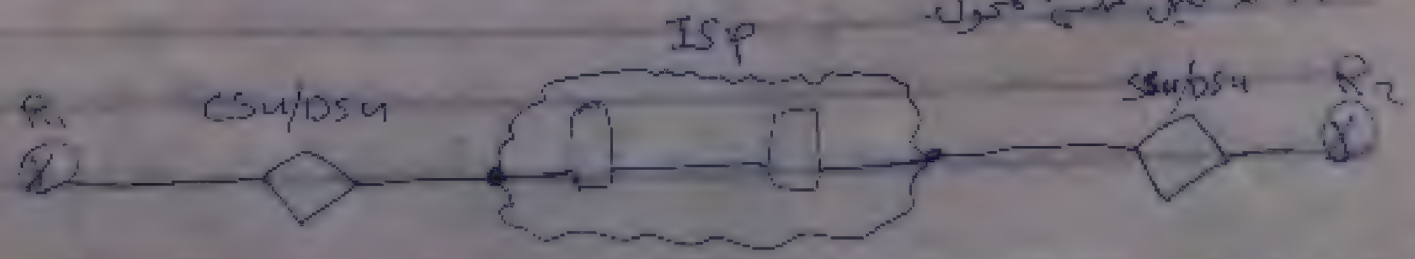
# Wide Area Networking WAN

تتكون الـ WAN من شبكات النفاذ التي تقدم البنية التحتية الممولة أو مشتركة  
من طرف مزود الخدمة المتنازعة وتربط بين مناطق جغرافية.



- ① Customer premises equipment (CPE)
  - المقصود بالأجهزة التي تتواجد عند العميل وليس شركة الاتصالات أو ISP مثل DSL Modem
  - مشيرة إلى الأجهزة
- ② Demarcation point.
  - وهو الأجهزة أو المنطقة التي تنقسم فيها أجهزة العميل (CPE) وتبدأ خطوط شركات ISP عندها مكان الجهاز اسفل المنبر المعلق به كابل الهاتف
  - مثلا PSTN هو يركب اسفل المنزل في public switched telephone network
- ③ Local Loop
  - المقصود بكابل التوصيل بين المستقر والسويش حيث يوزع
  - الخطوط المنبر وطولها ~~في PSTN~~ ~~على كابل يركب اسفل كبر~~
- ④ Central office (CO)
  - المقصود به شركة ISP أو مستقر الهاتف

⑤ CSU/DSU Channel Service Unit - Digital Service Unit  
جهاز يتم تحويل التيار به لتتم الخروج منه على شكل كابل هاتف وانعكس  
في النهاية على شكل كابل محمول



صندوق: 491/1  
رقم: 491/1  
تاريخ: 491/1

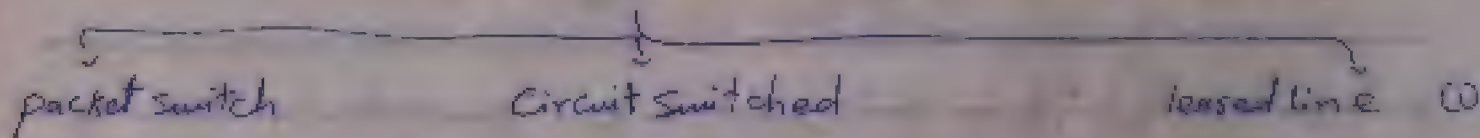
DTE 31-06E 31

1. **QPSK** هو اختصاراً لـ **Quadrature Phase Shift Keying** هو التقنية المستخدمة في  
 الاتصالات بين محطات البث واستقبال المخصصة لخدمة **ISG** وهي المسنونة  
 مع إشارة **CP Clock Rate** ترانسميتر/وإشارة المخصصة لخدمة **ISG**

DTE هو الجانب من الكابل الذي يتصل بالبروتوكولات في الطرف الآخر من الكابل  
Data Terminal equipment

## WAN Connection Types

التي هي التي أتت بها - أقامها - دأبها



leased line dedicated

٥  
٦  
٧  
٨  
٩  
١٠  
١١  
١٢  
١٣  
١٤  
١٥  
١٦  
١٧  
١٨  
١٩  
٢٠  
٢١  
٢٢  
٢٣  
٢٤  
٢٥  
٢٦  
٢٧  
٢٨  
٢٩  
٣٠  
٣١  
٣٢  
٣٣  
٣٤  
٣٥  
٣٦  
٣٧  
٣٨  
٣٩  
٤٠  
٤١  
٤٢  
٤٣  
٤٤  
٤٥  
٤٦  
٤٧  
٤٨  
٤٩  
٥٠  
٥١  
٥٢  
٥٣  
٥٤  
٥٥  
٥٦  
٥٧  
٥٨  
٥٩  
٦٠  
٦١  
٦٢  
٦٣  
٦٤  
٦٥  
٦٦  
٦٧  
٦٨  
٦٩  
٧٠  
٧١  
٧٢  
٧٣  
٧٤  
٧٥  
٧٦  
٧٧  
٧٨  
٧٩  
٨٠  
٨١  
٨٢  
٨٣  
٨٤  
٨٥  
٨٦  
٨٧  
٨٨  
٨٩  
٩٠  
٩١  
٩٢  
٩٣  
٩٤  
٩٥  
٩٦  
٩٧  
٩٨  
٩٩  
١٠٠

Can't switch C

موضوع آخر من طرز الاتصال تكونه بطريقه من صفة السرقة لكم ليزها امنه انتم فقط



ISDN 2B30 Disrupts service to 2B30 and 2B30

[illegible]

ISDN هي صيغة تفرقة الى 4 مداخل 2 مخرجين أو 2 مداخل 4 مخرجين فقط  
وهذا يضيق جهاز مع شرائط و تقوم -ترة الاتصالات بتزويدك بخدمات الانترنت بوقت  
الجهاز بتقسيم اللابيل الرئيسي الى جزئين جزء خاص بالملفات - الصوتية والآخر خاص بالملفات  
عامة فكل ما لا تترتت يتم توصيله بالكمبيوتر وتكونه -سرعة الانترنت في الوصلة التي قبل  
بجهاز الكمبيوتر 4Kbps وتقلية الاستغارة من 128Kbps الى 2Mbps  
لعدم الاستغارة من جهازها الخاصة

• بالانجليزية البرمجيات تكون ذات الاختصاص في Circuit switching

X.25. { ppp } Frame-relay - ATM.

و ATM باختصار، هو بیرونی و قوالب به سطح نقل و جمع اشیاء الیادتا کی video & voice مینرنا.

## packet switching - 3

فكره انه هو خليفة سيم مميزات التلغيم التقليدية مثل Circuit switching والسريعة العالية  
مثل leased line. ويقيم فيه جهاز DSLAM Digital subscriber line access Multiplexer  
نغني انه خطوط ADSL هي خدمة انترنت مبنية على خطوط الهاتف وتقوم بحمل البع  
هذه جهاز DSLAM يتم وضعه في المنزل او محل العميل خطوط الهاتف مدمجة  
ثم تخرج من الجهة الاخرى خطوط ADSL ياخذ الوسيلا واحد مدمجاً مثلاً لم يفتح بتوزيعها  
على المشتركين وتكون السرعة بنطاق 1:8 او يقيم نظام ال packet switching بروتكول  
مثل PPP وال Frame relay

مجموعة protocols التي تعمل على نقل البيانات عبر الشبكات المحلية (LAN) أو الشبكات الواسعة (WAN) أو الشبكات اللاسلكية (Wireless).  
 \* ADSL: Asymmetrical DSL. هي تقنية اتصال بالإنترنت تستخدم خطوط الهاتف النحاسي. تتميز بسرعات تحميل عالية (Download) وسرعات إرسال منخفضة (Upload).  
 \* SDSL: Symmetrical DSL. هي تقنية اتصال بالإنترنت تستخدم خطوط الهاتف النحاسي. تتميز بسرعات تحميل وإرسال متساوية.  
 \* VDSL: Very High Speed DSL. هي تقنية اتصال بالإنترنت تستخدم خطوط الهاتف النحاسي. تتميز بسرعات تحميل وإرسال عالية جداً.

ADSL	SDSL
Asymmetrical DSL	Symmetrical DSL
تكون فيه سرعة الـ Download أكبر من سرعة الـ Upload	تكون فيه سرعة الـ Download مساوية لسرعة الـ Upload

## WAN protocols

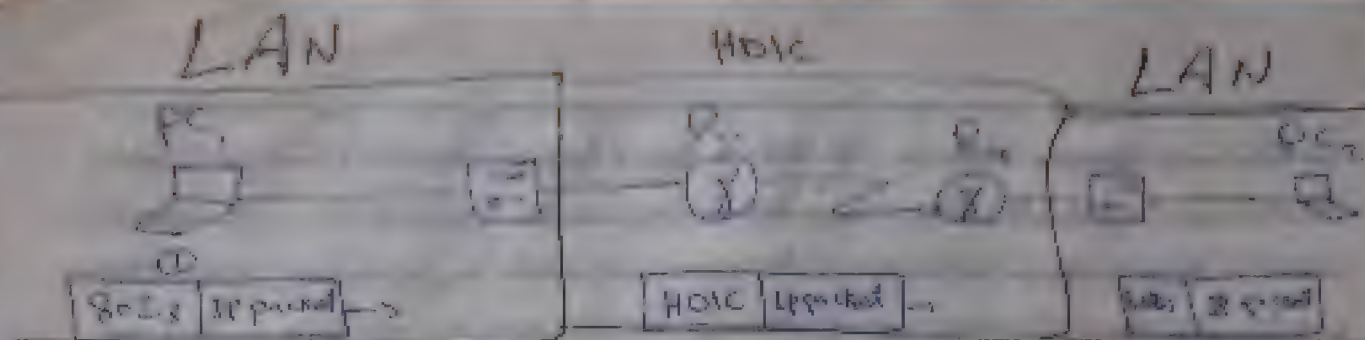
**HDLC** High Level Data Link Control  
 وهو بروتوكول Default على أجهزة سيسكو. لا يحتاج لضبط على أجهزة سيسكو. ينقسم إلى نوعين HDLC Cisco وهو فقط التشغيل على أجهزة سيسكو وضع آخر HDLC ISO ويعمل على الأجهزة الأخرى مثل أجهزة سيسكو.

نقطة انطلاق



في حالة إرسال A إلى B، فإن الـ Frame يرسل إلى B. عند وصوله إلى B، يتم فك التغليف (decapsulation) لإزالة الـ mac address. عند إرسال B إلى A، يتم فك التغليف لإزالة الـ mac address. في حالة إرسال A إلى C، يتم فك التغليف لإزالة الـ mac address. في حالة إرسال C إلى A، يتم فك التغليف لإزالة الـ mac address.





في حالة تزايد السيرفيس التي تقدمها الشركة في حال تزايد عدد العملاء في الشركة  
 يتم استئجار خطوط ISP خاصة به الشركة التي تملكها الشركة التي تملكها الشركة  
 ولا يتم بالتصميم الاستئجار وبالعالم - تقدم الشركة التي تملكها الشركة التي تملكها الشركة  
 أفضل من ذلك هو Tunneling وتلك هي الطريقة التي تملكها الشركة التي تملكها الشركة

لا يمكن استخدام هذه الأجهزة المختلفة

عيبها HDLC

لا يتم عليه التشفير أو Authentication ولا تتحكم في leased line

مميزته ① أسهل في الاتصال والتفصيل على أجهزة - يمكنه بأنه By default وهو بسيط  
 وبالنسبة إلى الأجهزة غير يمكنه فتح فقط ضبط ال encapsulation وقد نزلها

HDLC

هو بروتوكول HDLC هو البروتوكول الأسرع على الأقلام حيث يتم ال Header صغير  
 من ال packet

## ② بروتوكول ppp

PPP هو اختصار point-to-point نتفخ منه أنه لو وصل فقط فيه بسيط جداً  
 كل HDLC ويعتبر PPP أكثر البروتوكولات - تحتها ما في العالم كونه أنشأه مستخدم  
 الإنترنت يعتمد على الوصول إلى الإنترنت من خلال الاتصال مع شركات ISP والتي تتم  
 خلال بروتوكول PPP وتكون هذه PPP أيضاً أنه يستطيع العمل مع أجهزة الراوترات  
 المختلفة بخلاف HDLC فالنوع لا يسمح بأجهزة وشركات مختلفة.

ينقسم بروتوكول PPP إلى

Link control protocol [LCP]

Network Control protocol [NCP]

هذه هي مميزات **Link Control Protocol (LCP)** في بروتوكول الشبكة: **Link Control Protocol (LCP)**  
 1. إنشاء وصلة بين النقطتين المتصلتين. وهذا يتم من خلال التفاوض على المعايير  
 negotiation مع الطرف الآخر للتأكد من أن كلا من طرفي الاتصال يتبعان المعايير نفسها  
 وهذا المعيار يوضح كيفية التعامل بالتفصيل وهو على شكل ملف تعريف **Dot-Link**

Link Quality Monitoring (LQM)	يتم فيه تبادل الإحصاءات حول نسبة الضيق التي وصلت نسبة أخطاء
Looped Link detection	يقوم <b>LCP</b> بتوليد رقم عشوائي يسمى <b>magic number</b> يرسله أربع مرات بلطفه الهيكلي ويتم إرساله في حال استلم هذا الرقم مرة أخرى بعد إرساله أنه يوجد <b>Loop</b> وبالتالي يتم إيقاف الاتصال
Layer 2 load balancing multi link	يتم فيه التفاوض مع الطرف الآخر من أجل توزيع الترافيك كما أنه لو كان هناك أكثر من لينك يصل النقطتين وبالتالي يستخدم خاصية الـ <b>loadBalancing</b>
Authentication	وهو من أجل التأكد من الوثوقية والتوافق بين النقطتين وهذا يتم من <b>chap</b> و <b>pap</b>

هذه هي مميزات **Network Control Protocol (NCP)** في بروتوكول الشبكة: **NCP** ②  
 1. **encapsulation** بين النقطتين وبالتحديد إدارة بروتوكولات  
 الطبقة الثالثة **Network**

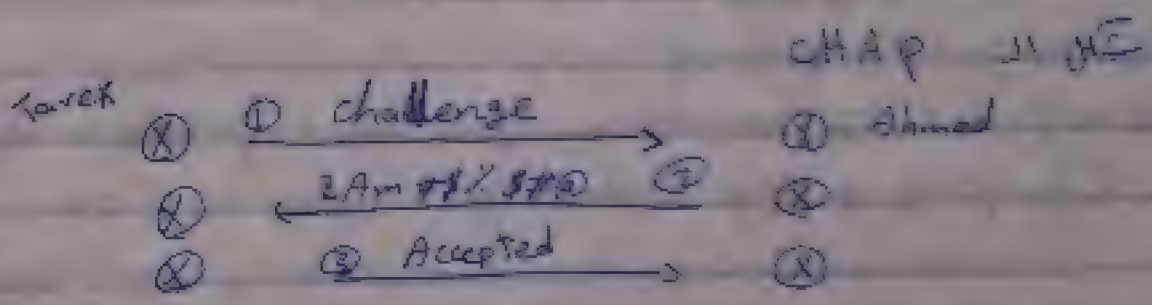
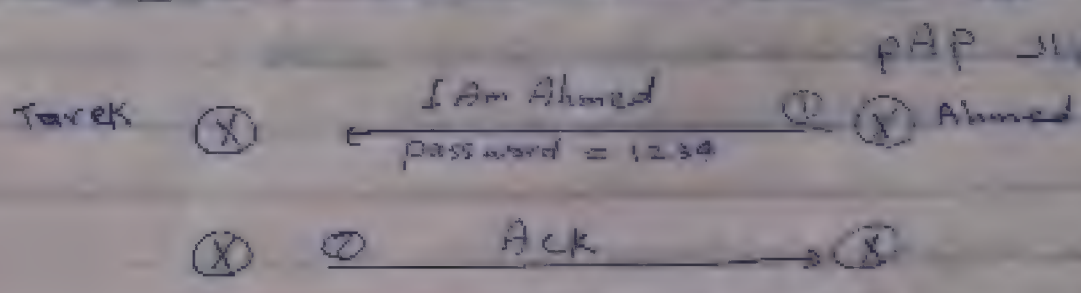
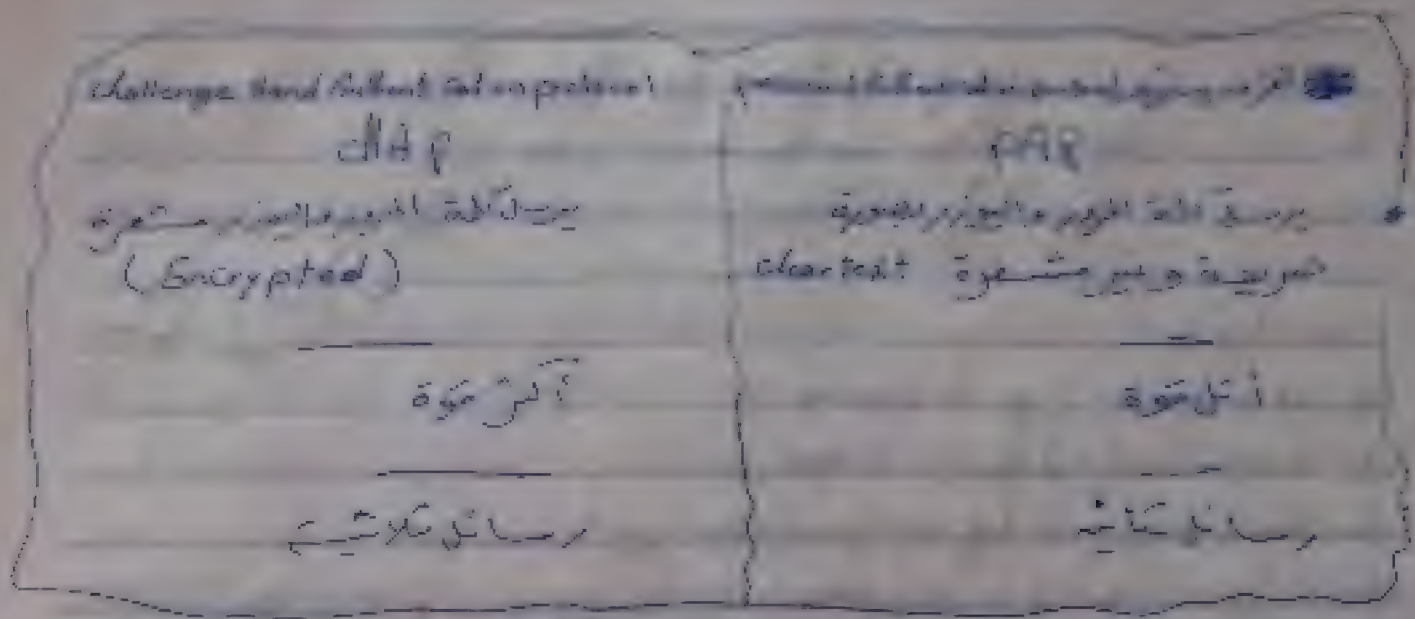
## Authentication protocols

تنقسم بروتوكولات التوثيق إلى نوعين

CHAP

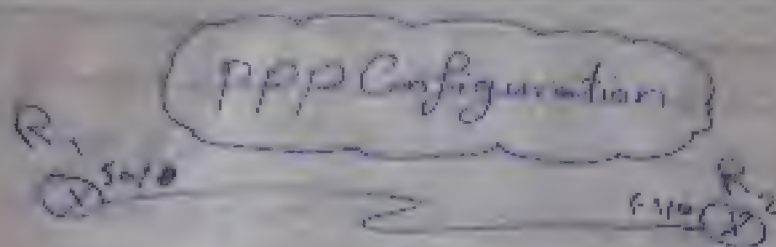
PAP





\* بروتوكول PAP يعني يتأكد هذا البروتوكول من المصداقية الأساسية طلب التوثيق Authentication Request  
 يرسل الجهاز المتأ للوقفل طلب توثيق فيه اسم وأقدم كلمة مرور (2) رد التوثيق  
 Authentication reply فيجيبه الجهاز الآخر بما إذا كان سيقبل الجهاز الأول المقدم للمستخدم  
 كلمة المرور

\* بروتوكول CHAP يعني لا يرسل كلمة المرور وإنما يقوم الجهازين بتطبيق عملية حسابية  
 لكلمة المرور ومن ثم التأكد من نتيجة هذه العملية للتأكد من مطابقة كلمة المرور



Router 1

CHAP ①

```
Router (config) # hostname R1
Router (config) # int Serial 0/0
Router (config-if) # encapsulation ppp
R1 (config-if) # username + أحمد + password 123
R1 (config-if) # PPP Authentication CHAP CHAP
```

R2

```
Router (config) # hostname R2
Router (config) # int Serial 1/0
R2 (config-if) # encap ppp
R2 (config-if) # username + أحمد + password + 123
R2 (config-if) # PPP Authentication Chap
```

PAP ②

password 123 chap أحمد أحمد أحمد

R1

```
Router (config) # hostname R1
R1 (config) # int serial 0/0
R1 (config-if) # encap ppp
R1 (config-if) # ppp Authentication PAP
R1 (config-if) # ppp PAP sent-username
R1 password 123
```

R2

```
Router (config) # hostname R2
R2 (config) # int Serial 1/0
R2 (config-if) # encap ppp
R2 (config-if) # ppp Authentication PAP
R2 (config-if) # ppp PAP sent-username
R2 password 123
```



Router # debug ppp negotiations

Router # debug ppp packets

Router # debug ppp errors

Router # debug ppp authentication

Router # show interfaces serial 0/0/0

حالة التهيئة التي لا تتوفر قد لا تتوفر احد الطرفين

ملاحظة: يجب ان يكون الطرف الآخر هو الذي يكون عليه الوضع

Router (config) # ppp authentication chap ppp

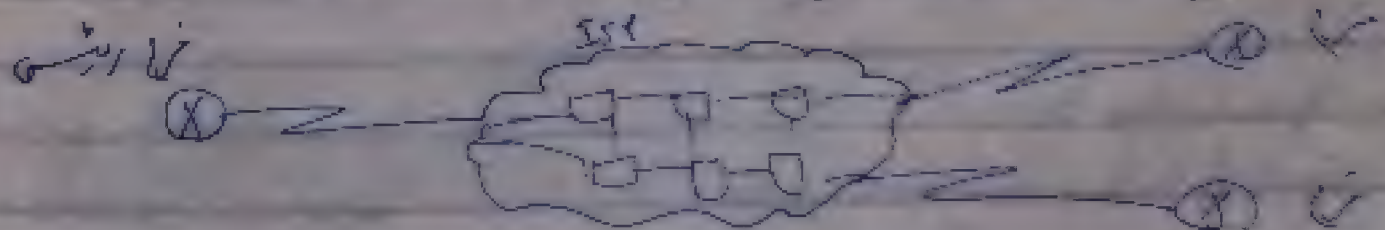
## Frame Relay

تقنية الـ Frame relay هي خدمة تقدمها شركات ISP للشركات والمؤسسات المختلفة  
عبر خطوطها لتستطيع تلك المؤسسات ربط أكثر من فرع إلى نقطة مركزية واحدة مثل  
المبنى. وتعتبر تقنية الـ Frame relay من أشهر تقنيات الشبكات المقدمة الـ WAN  
وهي تتمتع بالآتي:

① رخصة الـ leased line مقارنة بخطوط الـ leased line

② Shared Bandwidth

ملاحظة: تتكون لشبكة الـ Frame relay من فرعين رئيسيين وفروع فرعية يتم الربط بينهم  
من طرف المؤسسة التقنية لشركات ISP



\* الأجزاء من الـ ISP الخاصة بتقنية الـ Frame relay قسم الـ Frame relay هو قسم  
أو نقطة يتم عبرها نقطة الأمان التي تسمح أنه يكون الفرع الرئيسي والفروع الأخرى  
مستقلة واحدة.

# مقدمة عامة

تتميز شبكة البيانات بخاصة مبردة على مستوى التوزيع والتركيبية  
 من حيث التوزيع والتركيبية حيث أن الشبكة تتكون من عدة  
 أجزاء مترابطة مع بعضها البعض ويتم ربط الفروع الرئيسة مع فرع واحد فقط على الإنترنت



المسار من القاهرة لا يمكنه من الوصول إلى مصر القاهرة لظهور مسار  
 ويحتاج آخر سير للأحمال و... أهمية لأنه من الأفضل هذه المسارات لم يتم تخصيصها  
 لهذه الفروع والفروع الرئيسة حيث أنها تستخدمها شركات الـ ISP لتربط  
 المناطق ببعضها وتم استخدامها على طريقتين المسارات الـ Config لتربط  
 فروع القاهرة باستندرج والقاهرة بطنطا وفناء من الوصل تربط فروع حتركا أخرى  
 فخصيص الـ lease line لا يمكنه أن يستخدمه أو شركته أخرى غير الشركة  
 المقابلة عليها هذه المسارات الوهمية تسمى PVC - يمكنه من لا حقا

• نلاحظ من الشكل أنه الـ Frame relay عبارة عن جزئيين الـ Cloud و...  
 عن المسارات هذا الجزء هو شركة ISP ويتم دراسة هذا الجزء من...  
 • وأما الجزء الآخر فهو روترات المركز الرئيس والفروع المختلفة وهو ما نتناوله - مقدمة  
 CCNA & CCNP Routing and Switching

## # Frame-relay encapsulation #

الرافعة يكونه مفتاح الـ HDLC encapsulation من البساطة ولكن تفعل عليه تقنية  
 الـ Frame-relay نحتاج إلى تفعيل الـ Frame-relay encapsulation عليه وتقسيمه إلى

5	
encapsulation IETF	encapsulation Cisco
تربط بين روترات	تربط بين روترات

## # PVC #

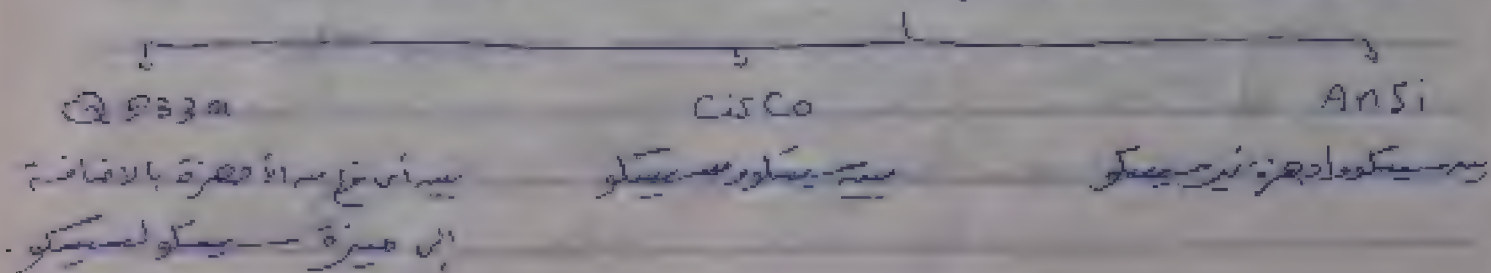
هو افتراضي permanent virtual circuit وهو عبارة عن المسارات الوهمية



[illegible]

# (LMI) #

هو الواجهة Local management interface وهو عبارة واجهة التعامل مع الواجهة  
والـ FR switch وهو يتحكم بتغيير الـ Bandwidth وتوزيعه على المنافذ المتصلة  
بالتسليم الرئيسي بصورة مستقلة مع انه من الممكن ان يكون قابلاً للتعديل عند الحاجة  
حيث يتم الـ LMI

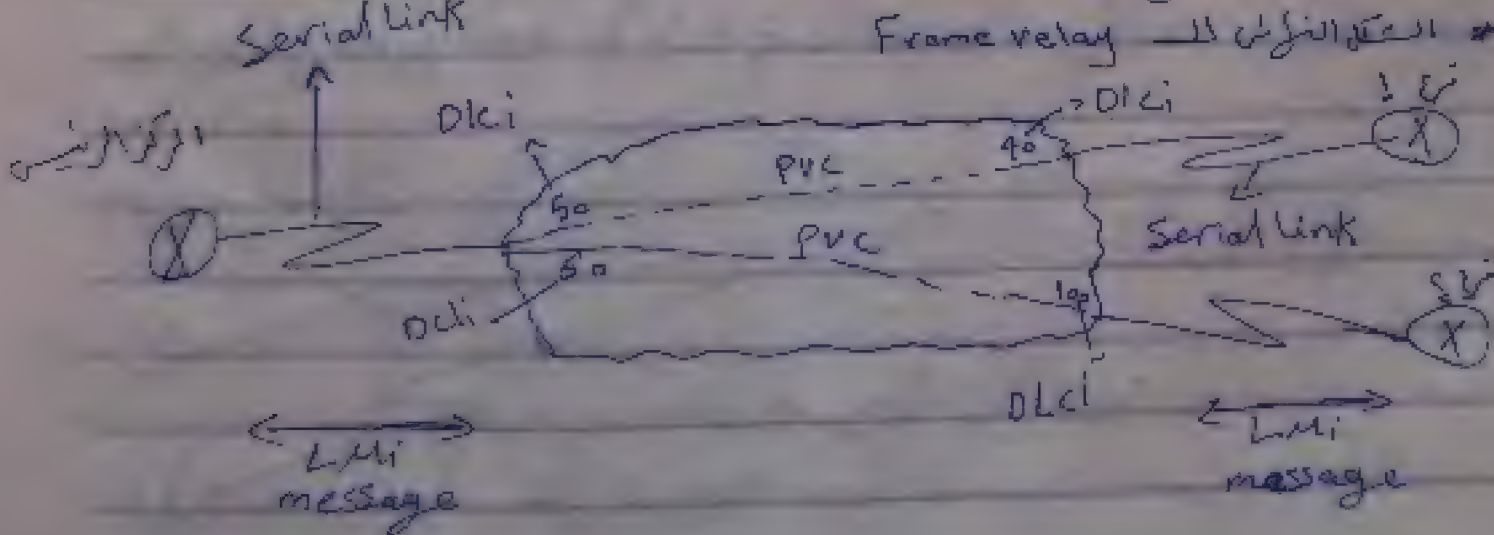


Committed information rate # CIR #  
Primary information rate # PIR #

# DLC: #

هو رقم تعريف للمحرقة يتم تحديدها بالمار الفند مستقرية العاتات

يتم وضع رقم الـ DAC على رأس كل مادة وهو PVC حيث يكون ضمن الاوراق  
منه 17 ويصل إلى 1000 لا يحتاج رقم الـ DAC وآخر عند المركبات الرئيسية وكله تدقيقه  
رقم الـ DAC في الفرع

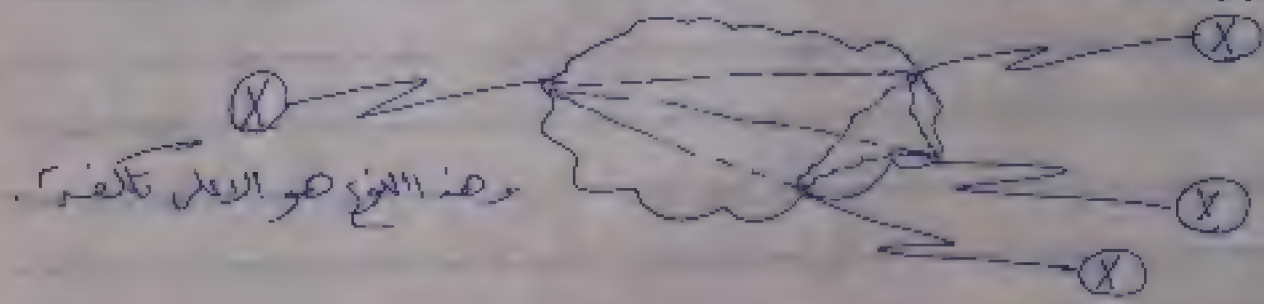


# Frame relay Topology

- ① mesh Topology
- ② partially Topology
- ③ hub and spoke

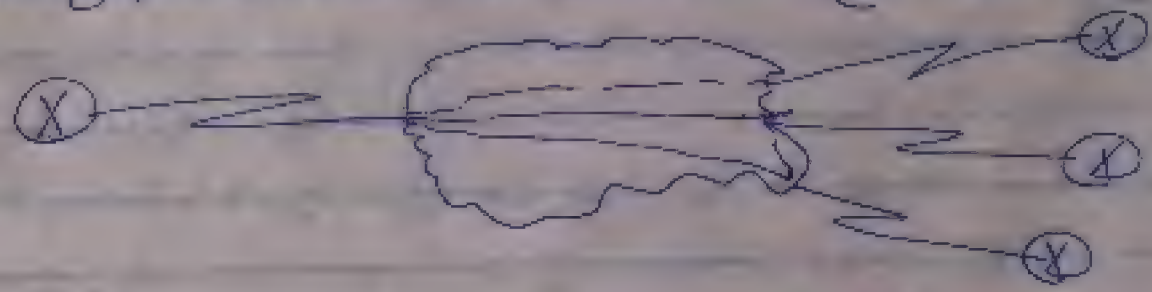
## ① Mesh Topology

من مميزات الشبكات mesh المركز الرئيسي مثل الفروع متصلة ببعض العقد الرئيسية كل فرع واحد فرعي  
كل فرع واحد فرعي الرئيسي PVC لا تتصل



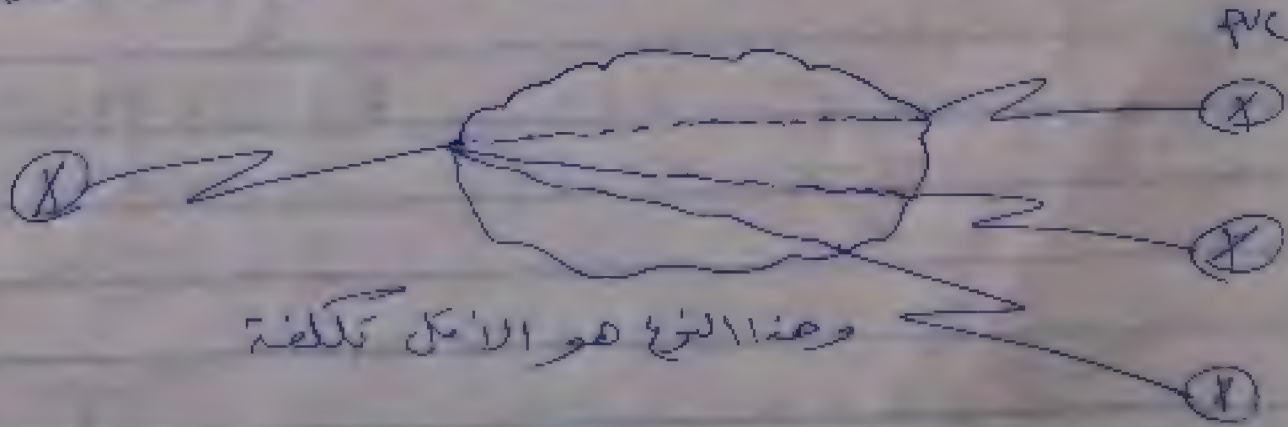
## ② partially Topology

من مميزات النوع ليس كل الفروع متصلة ببعض العقد الرئيسية PVC وتصل بعض العقد كذلك



## ③ hub and spoke

من مميزات النوع الفروع تتصل بالمركز الرئيسي فقط ولا تتصل أو لا يوجد بين فرعي رئيسي





Found - correct in figure.

تنقسم الـ Frame today إلى ٢ أنواعين الأول point to point ② والثاني point to multipoint ①

Point to multipoint ☒

من هذا النوع أخرج السيرة عند تطبيع السواحل مع بعض ما احتجنا من أصل مع  
الخرق الرئيسي بفتح واوهم والله

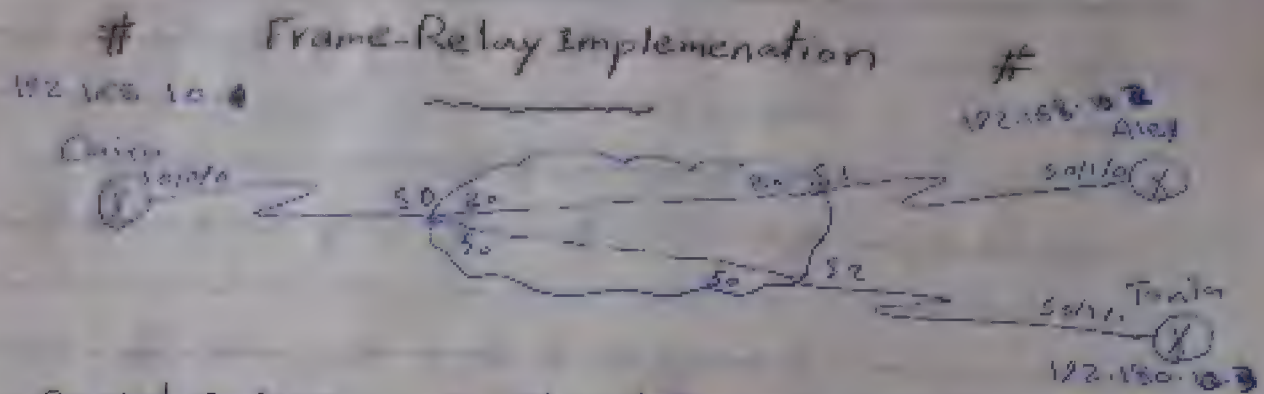


تلاحة الموزع الاستمرارية عند ملئها بالخواص مع حجم موزع لها فائدة لا بأس بها بل  
المركز الرئيسي هي كائنات لا يوجد PVC يعبئها الموزع وظيفتها هي استخراج  
البيانات إلى الموزع الرئيسي وتلك لا تخرج من النظام وذلك في صورتها المباشرة إلى  
مركز Split Node التي تتبع خروج البيانات إلى الـ Update من قبل الموزع إلى  
استلامها من البيانات أو الـ Update وبالتالي لا تستطيع الموزع من هذا النوع أن يعبئ  
أي شيء بفضل إلا إذا تآكل الـ PVC يربط الموزع ببعضه ويكتمل إلى PVC  
له تلكه من يجعل نوع multi point على التكلفة.

بعض لغات البرمجة "multipoint" تتلوه القزوع والد أير الرئيس عبارة عن تقسيم الشبكة  
إلى أقسام أصغر من فئة C أو شبكة واحدة من ال Subnetworks

point to point [c]

من هذا النوع يتم التقلب على خاصية الـ Split Horizon بطريقة تقسيم الترتيب  
إلى نظام Sub-interval وبالتالي تستطيع الفرع أن تتعامل مع بعض الأحداث  
وكل فرع يعتبر بمثابة فضاء به أن كل فرع له  $IS$  من حيثية غير متساوية  
لنظام بالفرع الآخر أو بالمرکز الرئيس وهذا النوع أقل تكلفة من الترتيب  
وبالتالي تفضل الشركات استخدامه



- Packet Tracer إلى Cloud إعدادات الـ (P) #####
- ① نذهب على برنامج الـ packet tracer ونضيف على الـ cloud ونختار Config
  - ② نذهب لـ interface ونختار البورت Serial 0 وهو متصل بالقاهرة
  - ③ نظهر الشاشة التالية

DLCI  Name

- ④ نكتب رقم الـ DLCI وما يقابلها من اسم الفرع مثال DLCI 20 واسم الفرع القاهرة
- DLCI  Name
- 

- ⑤ نكتب الـ DLCI الأخرى وما يقابلها ونضغط Add
- \* انتبهنا البورت Serial 0 فنختار بعده بورت آخر وتجميع قس الخطوات
- نضيف الـ DLCI وما يقابلها من الفرع

- ⑥ نضغط الآن على خيار Frame Relay الموجود في قائمة الخيارات في عمود الـ Config الخاص بالـ cloud
- \* تظهر لنا الشاشة

Serial 0  Serial 1

- Serial 0 نختار سيرال 0 ونختار اسم الفرع ثم نختار الـ Serial 1 بالفرع سقوة سيرال 1 ونختار الفرع الرئيس القاهرة أما إذا عرقلنا الـ سيرال 0 له إنشاء pvc طريق Alex ويقابل سيرال 1 الفرع سقوة
- نعمل Alex بالقاهرة. ثم نضغط Add لفرع الحبار



\* تكرر السطح نقطة Serial 0 تكرر السطح نقطة Serial 0  
 Serial 0 Tanta Serial 2 Cairo

مرتداد pvc الكاب - سيخرج لنقطة التي يصل بالقاهرة عبر فرع Serial 2  
 Add نقطة

== ## (ب) إعدادات الروايت  
 تنصب الآن تكرر راسيتن حيتيغ الذن

① Cairo

```
Router (config) # host Cairo
Cairo (config) # int s0/0/0
Cairo (config-if) # no shutdown
Cairo (config-if) # encapsulation frame-relay
Cairo (config-if) # ip address 192.168.10.1 255.255.255.0
```

② Alex

```
Alex (config) # int s0/1/0
Alex (config-if) # no shutdown
Alex (config-if) # ip address 192.168.10.2 255.255.255.0
Alex (config-if) # en encapsulation frame-relay
```

③ Tanta

```
Tanta (config) # int s0/1/1
Tanta (config-if) # no shutdown
Tanta (config-if) # ip address 192.168.10.3 255.255.255.0
Tanta (config-if) # encapsulation frame-relay
```

هذه الطرق تسمى طرق Frame-relay التي لا تحتاج إلى إعداد مسبق  
أمر `show frame-relay map` للتحقق

`Router# show frame-relay pvc`  
`Router# show frame-relay map`  
`Router# show frame-relay lmi`

### • فكرة map

فكرة أخرى أن نتطبع أنه أعلم الأستراتيجيات لكن يري الأستراتيجيات المقابل مع خريطة  
رقم الـ DLI الخاص به كنوع من زيادة التأكيد

مثال نرى في المثال السابق تأكيد أنه يري الأستراتيجيات 0/0/0 الخاص بالقاهرة في  
الأستراتيجية مع خريطة الأستراتيجيات 192.168.10.2 مع خريطة رقم الـ DLI الخاص به  
وهو 20 وإنا هنا أستاذ برامتر القاهرة - تياو والأمر كالتالي

رقم الـ DLI الخاص به + - - - - - الخاص بالأستراتيجيات IP # Frame-relay map ip  
المقابل

`Cairo (config-if) # Frame-relay map ip 192.168.10.2 20`

أمر الـ map هو أمر يربط رقم الـ DLI بعنوانه أي يربط رأس الأمر  
الذي يملكه مع خريطة بروتوكول IARP inverse address resolution protocol

### IARP

أولاً - الـ inverse ARP هو إضمار بروتوكول يقوم

بربط رقم الـ DLI بعنوانه IP المقابل أو بعنصر آخر يعرف

كل الـ DLI ما يقابل به عنوانه IP ويقوم بتدوير الأمر `show FR map` بأنه Dynamic  
فإنه يكتب أمر `MAP` يدور في رأسه أو رأسها Static

### أمر `# show FR LMI`

يستخدم الـ LMI لتقديم سوار

Cisco

Ansi

Q.933A

### أمر `show FR pvc`

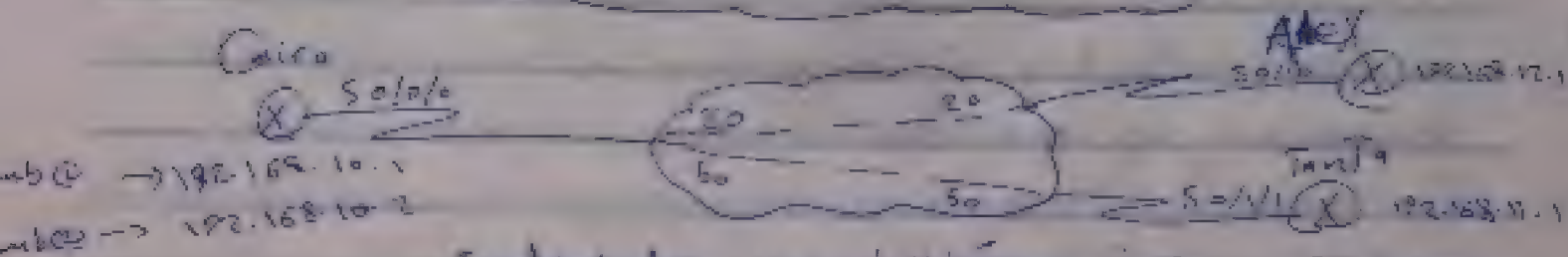
يستخدم الـ pvc للتحقق من الـ DLI ورقمه

ويعرف حالة الاتصال الـ pvc سوار



PVC status		
Deleted	Inactive	Active
حذف شده است	حذف شده است	حذف شده است
در حال حاضر در شبکه	PVC در حال حاضر در شبکه نیست	PVC در حال حاضر در شبکه است
	حذف شده است فقط در شبکه	حذف شده است فقط در شبکه
	حذف شده است فقط در شبکه	

## point to point Config



تقسیم کردن اینترفیس به ساب اینترفیس

① Cairo

فرمانها

Cairo(Config) # int S0/0/0:15 point-to-point

Cairo(Config-if) # no shutdown

Cairo(Config-if) # ip address 192.168.10.1 255.255.255.0

Cairo(Config-if) # encapsulation Frame-relay

Cairo(Config-if) # Frame-relay interface-dlci 20

تغییر نام IP در ساب اینترفیس DLci 20

بالنسبه للفرع لا نحتاج ان تقسمها الى Subinterface ولكن لا مانع ان نقسمها

نستطيع ان نرسل map الفعليه الى AR

Cairo(Config-if) # Frame-relay map IP 192.168.12.1 20 Broadcast

1 Mi Type

US-9330

Cisco

Cisco

مركز

Router (config-if) # frame-relay lmi-type lmi-type  
مع مراعاة أنه يتم تعيينه في جميع الروتينات إلى Topology ما عدا الـ Cisco  
في الـ Cisco فإنه By default يتعين الـ Cisco

Multipoint

خلاصة الاوامر

Router (config) # int S0/0/0

Router (config-if) # no shut

Router (config-if) # encap frame-relay

Router (config-if) # ip address

Router (config-if) # frame-relay lmi-type lmi-type

Router (config-if) # frame-relay interface-dlci DLI

point-to-point

Subinterface في interface

Router (config) # int S0/0/0.1 point-to-point

map

Router (config-if) # frame-relay map ip next hop + DLCI number ~~to~~ Broadcast

# show FR pvc

# show FR map

# show interface

# show frame lmi



## 4. Virtual Private Network (VPN)

الـ VPN هي تقنية لربط الشبكات البعيدة ببعضها بطريقة الآمنة حيث يتم إنشاء قناة آمنة يتم عبرها إرسال البيانات بطريقة مشفرة وتلعب الشركات لتأمين اتصالاتهم في العمل. أشهر من الأنظمة هي خدمات الـ leased line والـ frame-relay من حيث الأداء والاعتمادية. تقدم مميزات أداء وسرعة أفضل من الـ VPN.

4. الميزة الخاصة بالخصوصية (VPN) تقدم حل للمشاكل الأمنية التي تواجهها مقدمي الخدمات. حيث تقدم الأمن

① Confidentiality "privacy"

السرية أو الخصوصية حيث تقوم بالشفف أو تشفير البيانات غير مرغوب فيها عند قراءة البيانات والإفلاخ عليها وهذا الميزة من مميزات التشفير.

② Authentication

المصادقة. هي عملية التوثيق التي تضمن لنا أنه الطرف الآخر من VPN هو الطرف المقصود. فلا يمكن أن يتظاهر بأنه الطرف الآخر.

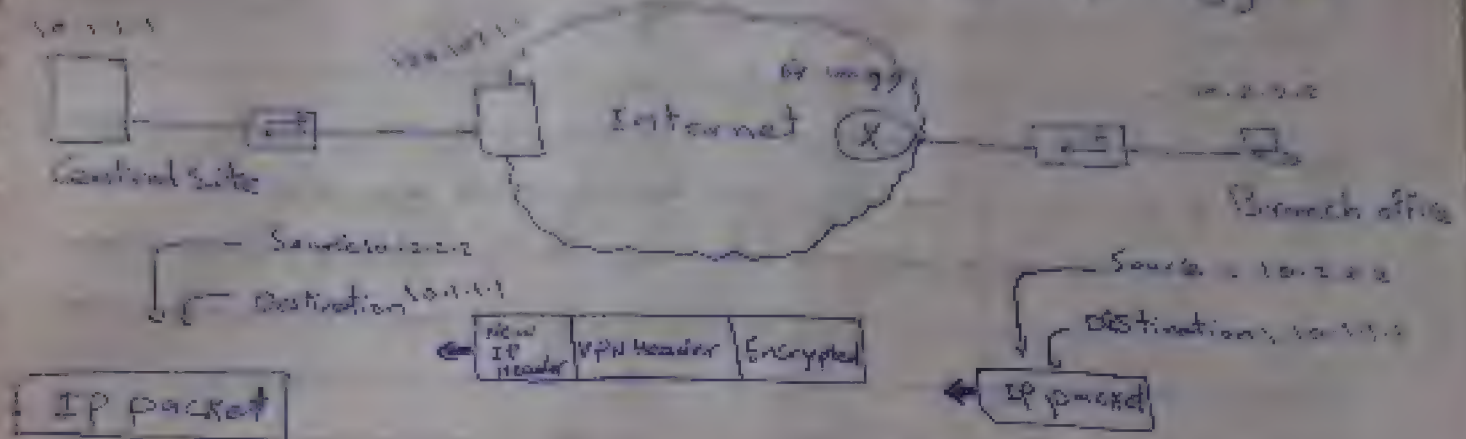
③ Data integrity

سلامة البيانات. هذه الميزة تضمن لنا أنه لم يتدخل طرف خارجي وقام بتغيير أو تعديل من البيانات المرسلة. وهذا الميزة من مميزات التشفير. #

④ Anti-replay

منع إعادة الإرسال. وهو يمنع المهاكر من نسخ البيانات وإعادة إرسالها مرة أخرى. حيث لا يمكنه أن يفعل لأنه استقبلها مرة واحدة سابقاً من القائل لا يستطيع إعادة إرسالها. التي تقوم بإرسالها مرة أخرى. هذا الميزة من مميزات التشفير.

## == VPN Topology ==



## Types of VPN

### Remote Access

يتمتع لاصحابها الشركة بالدخول من  
بعد إنشاء الشركة - عادة  
البيت أو أي مكان آخر

### Site to Site

يربط بين موقعين للشركة على الإنترنت الرئيس  
ملاصق فرع الشركة الأخرى

### Intranet

تتميز بجميع أجهزة الكمبيوتر الخاصة  
بموقعية مضمونة لتفحص الشركة

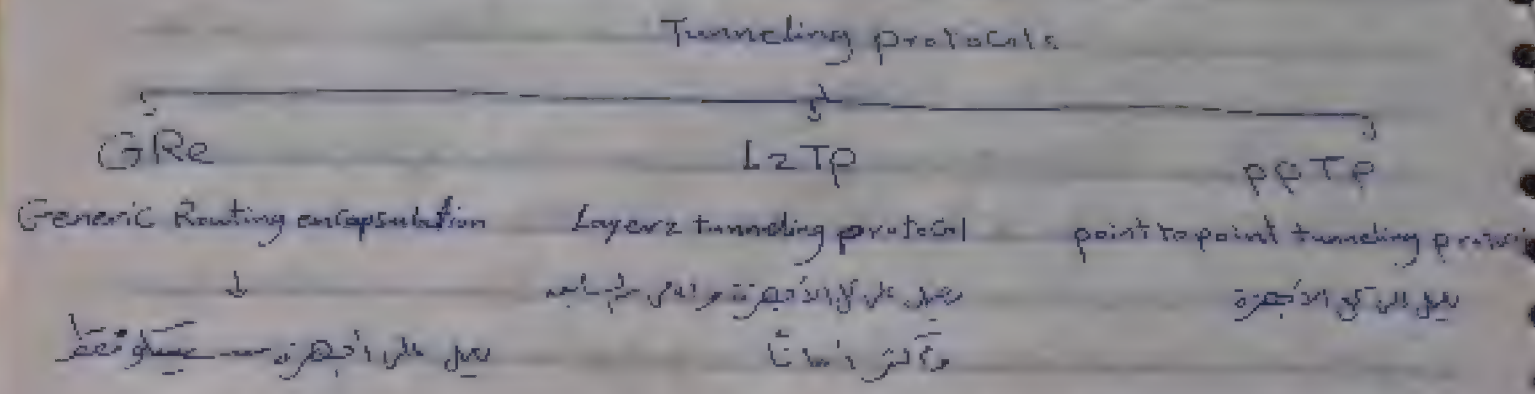
### Extranet

يربط جميع أجهزة الكمبيوتر الخاصة  
بموقعين لشركات مختلفة التي يتوفر  
شراكات أو مبيعات مشتركة وملاصق

## VPN Tunnel

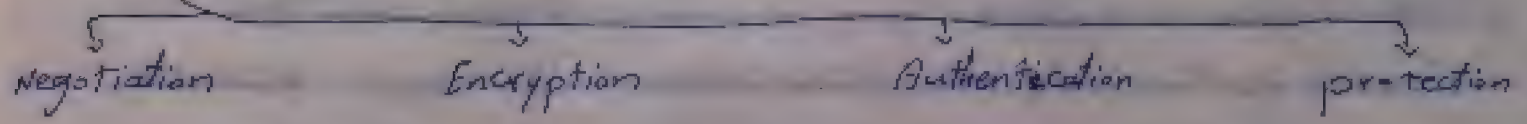
تُعرف الـ VPN الرئيسية كعبارة عن بناء نفق خاص بين جهازين أو المركز الرئيس  
والفرع. هذا الـ Tunnel أو النفق يتم تبادل المعلومات بصورة آمنة وصغيرة  
يتم إنشاء هذا النفق (Tunnel) خلال شبكة الإنترنت - ليتم نقل البيانات





# IP Sec

هو اختصار ← IP Security يقوم ال IP Sec بعمل 4 أشياء



لها مبادئ التفاوض التي تتم بين المكون الرئيسي والفروع والبروتوكولات المستخدمة هي AH و Esp أو Esp + AH

Negotiation [ ]

والأخير هو التوافق

البيانات التي تتبع الرسالة لا تتبع الرسالة plaintext ولأنه تكون رسالة لا يعرف محتواها إلا إذا تم فك تشفيرها والبروتوكولات المستخدمة هي

Encryption [ ]

مبادئ التشفير هي

① DES ← Data encryption standard ← يغير الحرف ب 56 Bit

② 3Des ← Triple Des ← الحرف يغير ب [3 x 56 Bit] 168 Bit

③ AES ← Advanced encryption standard ← يغير الحرف ب 128 و 192 و 256 Bit

④ JES ← يستخدم 128 Bit للتشفير الحرف

### Authentication

المصادقة والتحقق من هوية الطرف الآخر  
أهم ذلك هو القول به مصادقة الـ Authentication هي بروتوكولات  
MD5 أو SHA

### Protection

والقول به توفير الـ protection هي بروتوكولات  
DH<sub>1</sub> < DH<sub>2</sub> < DH<sub>3</sub> < DH<sub>4</sub>

بعد ما عرفنا ما يقوم به IPsec لابد ان نفهم انه يعطي عند تنفيذ حزمة من البروتوكولات  
في موقع [الترانس فير] لابد ان نفعلها على الموقع الآخر [الفرع] حتى نقوى بابتداء  
الـ Tunnel فيشكل - ليتم وذلك فلهذا قطع اشارة الـ Tunnel

صال

اذا فعلنا من المركز الرئيسي هذه الخزمة

① negotiation → ESP

② encryption → 3DES

③ Authentication → MD5

④ protection → DH<sub>2</sub>

اذا فعلنا هذه الخزمة فلابد ان نفعلها على الطرف الآخر حتى يتم ابتداء الـ Tunnel

بعد ارسال الـ data يتم عليه encapsulation لـ data وتضاف عليه مجموعة من الاضافات  
تشكل الـ data المستفزة و VPN Header ونيرها. وبذلك يتم عملية تأمين الـ data.

### Types of Encryption Keys

Symmetric  
Asymmetric

ينقسم التشفير الى نوعين

① Symmetric "متماثل"

نقل السر المستفزة في التشفير وذلك التشفير واحدة ويحلها كل من المرسل

والمتقبل و يستخدم فها هذه النوع [Des - 56 Bit] أو [3DES - 168 Bit] أو

Aes . 128 , 192 , 256 Bit



## Asymmetric

الذي يستخدم فيه مفتاحين مختلفين أحدهما للتشفير والآخر لفك التشفير وهذا النوع لا يحتاج إلى الاتصال المباشر بين الطرفين

نوعيه Keys - 1 Public Key - 2 Private Key  
 Public Key يكون مع كل الناس والPrivate Key لا يعرفه إلا صاحبها فقط

مثال: 3 أنواع A B C عند ما يرسل A إلى B فائدة لا يفهمها B

بواسطة Public Key بالفتح B ويرسلها B ويقلها بPrivate Key التي لا يملكها B وبالتالي يصل إلى A لو حاول C فكها فلهذه البيانات لا يستطيع لأنه لا يملك الPrivate Key الخاص بالفتح B وهكذا  
 ويستخدم من هذا النوع Asymmetric

DH نوع التشفير يبدأ بـ 512 إلى مالا يتعدى 1024  
 RSA يبدأ بـ 768 إلى مالا يتعدى 2048

## Authentication, verifying, Identifies

نوع استخدام أو تفعيل الAuthentication بطريقة

### PSK (pre-shared keys)

كل عبارة مع كلمة سر واحدة يتم بها التشفير  
 وتستخدمها جهة الاطراف ويخبر الطرف الآخر بذلك  
 شفرة بنفس كلمة المرور وعند التوافق يتم الاتصال  
 بين الطرفين والسماح للجهاز بالدخول للشبكة  
 أو جهة أخرى السواحل على الطريقة الأخرى

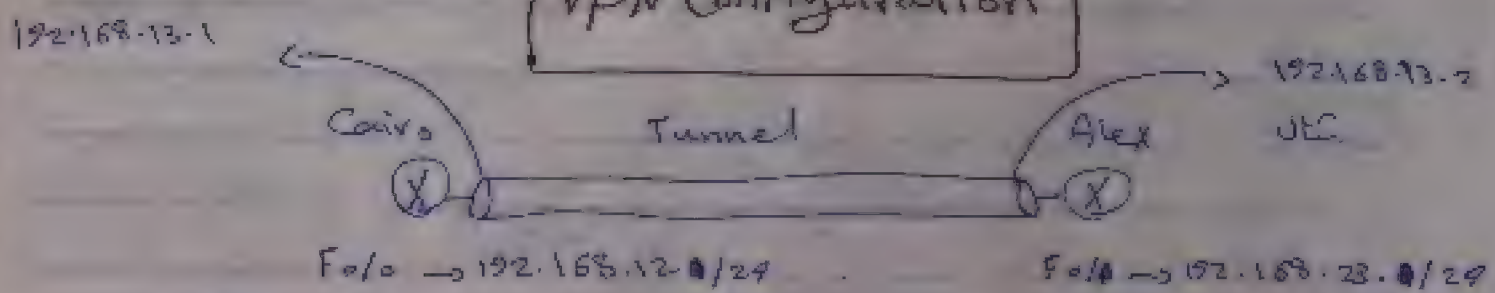
### PKI (public key infrastructure)

يقوم هذا النوع بإنشاء ما يسمى  
 Certificate Authority  
 كل جهاز يحمل اسم الجهاز والتشفير ومفتاح  
 التشفير وتحت إدارته ومفتاح البيانات التشفير  
 لهذه البيانات تعمل على توصيل كل  
 الطرف المتصل هذه الشبكة وإذا لم يتوافق  
 يتم الاتصال ولكن إذا كان هناك اختلاف  
 لا يستطيع إنشاء Tunnel

**Data integrity**

هذه خاصية من خصائص البيانات من التشفير بالبيانات  
 من خلال استخدام خوارزمية Hashing حيث  
 هذه الخاصية من البيانات المرتبطة مع البيانات المدخلة من خلال خوارزمية Hashing  
 أنه على الرغم من أن البيانات المدخلة قد تتغير ولكن الناتج من خوارزمية Hashing  
 لن يتغير لأن خوارزمية Hashing هي خوارزمية رياضية  
 يربط البيانات بترقيم على أن Hashing للبيانات من خلال خوارزمية رياضية  
 128 Bit ← MD5 ①  
 160 Bit ← SHA ②

# VPN Configuration



**Cairo**

```
Cairo(Config) # int Fa/0
Cairo(Config-if) # ip address 192.168.12.1 255
255.255.0
Cairo(Config-if) # no shutdown
Cairo(Config-if) # exit
Cairo(Config) # interface Tunnel 1
Cairo(Config-if) # ip address 192.168.13.1
255.255.255.0
Cairo(Config-if) # Tunnel mode GRE ip
Cairo(Config-if) # Tunnel Source Fa/0
Cairo(Config-if) # Tunnel destination 192.168
.13.2
ospf or Eigrp
```

**Alex**

```
Alex(Config) # int Fa/1
Alex(Config-if) # ip address 192.168.23.2 255
255.255.0
Alex(Config-if) # no shutdown
Alex(Config-if) # exit
Alex(Config) # interface Tunnel 1
Alex(Config-if) # ip address 192.168.13.2
255.255.255.0
Alex(Config-if) # Tunnel mode gre ip
Alex(Config-if) # Tunnel Source Fa/1
Alex(Config-if) # Tunnel destination
192.168.13.1
وتنقل البيانات من خلال الإنترنت
```

Show # Show interface Tunnel



# IPv6

تتكون عنوان IPv6 من 128 بت مقسمة إلى 8 quartet حيث أن كل quartet مكون من 16 بت وكل quartet يحتوي على رقم من 0 إلى 255 وكان عنوانه إلى 32 بت. يصعب لنا إيجاد عناوين IPv6 9.3 مليار جهاز تقريباً لكنه مع ظهور وسائل الاتصال هائلة تقام الإنترنت تزايدت وتدخل الأبحاث حول العالم بحثاً عن حلول أكبر مما أدى إلى نظام تلك العناوين. تلاءم الواجب الكفاءة طريقة جديدة للعنوان تعطينا مساحة أكبر من العناوين مع تزايد المشتغلين الذين يدخلون إلى شبكة الإنترنت يومياً. نتيجة لذلك قصر الأعداد الجديدة من عناوين IPv6 إلى 128 بت وهو ما يعادل 340 تريليون عنوان وهو عدد ضخم جداً حيث يمكن أن يكون المشتغل الواحد ما بين 5000 عنوان مما يدل على أن كل عنوان يحتاج إلى ترجمات والنتيجة المترتبة على ذلك هي الحاجة إلى ترجمات من الإنترنت إلى عنوان IPv6 مما يجعله غير قابل للاستخدام إلا في حالة الحاجة إلى الاتصال بالإنترنت أو الخروج للأنترنت من IPv6 على واحد "Public".

**شكل** يتكون عنوان IPv6 من 128 بت وينقسم إلى 8 quartet ومعنى quartet أي رباعي معناه أن quartet يحتوي على أربع أرقام سداسية عشرية (hexadecimal) أقل رقم سداسي عشري مكون من أربعة أرقام لذلك نجد أنه كل quartet هو عبارة عن 16 Bits. والأرقام السداسية عشرية هي من 0 إلى 9 ومن A إلى F بالتالي يكون شكل IPv6 كالتالي:

00AB : CF00 : 2934 : 1270 : 3210 : 4210 : 5611 : 877 : 991A

يفصل بين كل quartet خانة (:) وتسمى كونه

16 Bits = quartet \* كل

\* عبارة عن quartet 8

\* كل quartet = 4 أرقام hexadecimal أقل رقم = 4 Bits

\* الأرقام من 10 إلى hexadecimal من 0 : 9 + من A : F

\* إجمالي IPv6 = 128 Bits

\* بالعمل بدأ تطبيق IPv6 من قبل الدولة وتم إنشائه من عام 2001م ولذلك جعلوا العناوين التي تبدأ بـ 2001 هي العناوين إلى public وسيأتي الوقت الذي لن يكون فيه العمل بـ IPv6 ويتبدل كلياً للعمل بـ IPv6

## \* اختصار وتبسيط معاد 2946 \*

لاحظنا أن معاد 2946 معاد طويل حيث تكون به 10 أرقام  
 يتكون من أربع أرقام 0000 0000 وهو عنوان طويل حيث أن العنوان بطول العنوان  
 هذه الطريقة مع العمل عليه ذلك عبر طريقة اختصار العنوان أو دمج آخر تبسيطه  
 بعدة طرقه أمثلة (أصح طريقة)

### ① الطريقة الأولى

- من هذه الطريقة يتم الغاء الصفر على اليسار من اليمين إذا كان الرقم يكون مع حفر على  
 اليسار + رقم مثل 0008 هذه تخلصنا ⑧
- أيضا يتم اعتبار ال 0000 الذي كله الحفر تكتب حفر واحد فيلونه 0000  
 تكتب هكذا ⑤

### ② الطريقة الثانية

- من هذه الطريقة نستخرج فكرة حذف الصفر على اليسار من ال 0000 الذي  
 حفر على اليسار + رقم مثل 0008 تصبح ⑧
- أيضا يتم اعتبار ال 0000 التي كلها حفر وتكتب حفر واحد ثم  
 تكتب بعدها ② لكنه نراي أنه العنوان يسمح بوجود ② مرة واحدة فقط  
 مثال

1FE2 : 0000 : 0000 : ABCD : 0000 : 0000 : 0000 : 0058

(4) يتم اختصار هذا الرقم كالتالي حسب الطريقة الأولى

1FE2 : 0 : 0 : ABCD : 0 : 0 : 0 : 58

### (5) يتم اختصار هذا الرقم كالتالي حسب الطريقة الثانية

1FE2 : 0 : ABCD : 0 : 0 : 0 : 58

أو

1FE2 : 0 : 0 : ABCD : 0 : 58

ونلاحظ أنه ② تكررت مرة واحدة في العنوان حيث لا يمكن أن تأتي أكثر من مرة  
 وبالنسبة الشكل التالي خطأ

1FE2 : 0 : ABCD : 0 : 58 X

خطأ لأنه كثر ② أكثر من مرة وهذا لا يوجد إلا مرة واحدة فقط في العنوان



**IP mask** مثال: 255.255.255.0  
 أو صيغة أخرى: 255.255.255.0

**مثال:** 255.255.255.0 255.255.255.0  
 هي صيغة شبكة العنوان 255.255.255.0 أي

الخاصة

أما إذا كان mask هو 32 وبالتالي تقسمه على 8 Bits وتكون النتيجة  
 الرقم العاشر [الخاصة]  $32 = 4 \times 8$  أي 4 أجزاء

ويعرفها أنه أن quartet هو 2 أجزاء quartet = 32 أي أن quartet  
 الأول والثاني والثالث والرابع

255.255.255.0  
 255.255.255.0

وبالتالي كما نرى في الشبكة

**\* جدول التحويل من hexadecimal إلى Binary والعكس**

الترقيم الثنائية	hexa	Binary	hexa	Binary
0	0	0000	8	1000
1	1	0001	9	1001
2	2	0010	A	1010
3	3	0011	B	1011
4	4	0100	C	1100
5	5	0101	D	1101
6	6	0110	E	1110
7	7	0111	F	1111

وبالتالي يكون الرقم 128  $000100101000$  فمثلاً  $100000000 = 128$   
 وللتحويل من Binary نقسم الرقم إلى مجموعات كل مجموعة 8 أرقام فيكون الرقم  
 $000100101000 = 1000$   $0001 = 1$   $0010 = 2$   $1000 = 8$   $128$

## Types of Communication

① **Cast** : هذا النوع من الاتصالات هو الذي يرسل البيانات من جهاز إلى جهاز في الشبكة.  
 في هذا النوع من الاتصالات ونقطة البداية هي نقطة ونقطة النهاية هي نقطة.  
 وهذا النوع يستخدم في IPv4 و IPv6.

② **multicast** : هو النوع الذي يرسل البيانات من جهاز إلى مجموعة من الأجهزة وليس كل الأجهزة في الشبكة. يستخدم في IPv4 و IPv6.

③ **Broadcast** : هو النوع الذي يرسل البيانات من جهاز إلى كل الأجهزة في الشبكة. يستخدم في IPv4 و IPv6.

④ **Any Cast** : هذا النوع من الاتصالات هو الذي يرسل البيانات من جهاز إلى أقرب مسار متاح.  
 لو أنه سيرقات موقع يتوجب في ألمانيا وإيطاليا وأمريكا واليابان فإذن عند الاتصال بجسور يقوم بإختيار أقرب مسار وهو إيطاليا مثلاً ويعقد هذا أنه كل السيرقات مفضل عليها نفس عنوان ال IPv6 لكنه مع بعض ال Config التي تتلخص في تصادم ال بيانات . فتقوم فكرة ال anycast على اختيار أقرب مسار لهذا السيرفر.

## مصطلحات أخرى

① **unique local** : يقابلها في IPv4 **Local** وهذا النوع من عناوين يبدأ بـ FD...

② **Global unicast** : يقابلها العناوين ال public في IPv4 وهذا النوع من عناوين يبدأ بـ 2000 أو 3000

③ **multicast** : يبدأ بـ FF...

④ **Link local** : وهو عبارة عن العنوان الذي يأخذها الجهاز بشكل افتراضي في حالة IPv6 فما حاله إذا لم تعطى الجهاز عنوانه بشكل يدوي أو في حال لم يأخذ عنوانه من طريقه سيرفر DHCP فيأخذ عنوانه من ال APIPA وتكونه كالتالي 169.254.x.y والذي يقابله في IPv6 هو العنوان الذي



عنوان الـ Link Local هو FE80

$$\begin{array}{|c|} \hline \text{64 bits} \\ \hline \text{FE80} : 0 : 0 : 0 \\ \hline \end{array} + \begin{array}{|c|} \hline \text{64 bits} \\ \hline \text{EUI-64} \\ \hline \end{array}$$

عنوان الـ EUI هو عنوان الـ MAC

$$\text{EUI} = \text{first half of mac} + \text{FFFE} + \text{end half of mac}$$

مثال لو عنوان الـ MAC هو 1612.3456.789A

تكون الـ EUI هو 1612.34FF.FE56.789A

وتكون عنوان الـ Link Local هو

FE80 : 0 : 0 : 0 : 1612.34FF.FE56.789A

عنوان الـ Link Local هو الذي يتم الاعتماد عليه في IPv6 حيث في IPv6 لا يوجد

بروتوكول ARP الذي كان يقوم بمعرفة عنوان الـ MAC للأجهزة المتصلة في الشبكة

حيث في IPv6 يتم استخدام NDP ← Neighbor Discovery protocol الذي

يستخدم عنوان الـ Link Local مكان الـ MAC في برتوكول

## IPv6 MultiCast Addresses

① FF02 :: 1 → كل الأجهزة على الـ لينك التي تستخدم IPv6

② FF02 :: 2 → كل أجهزة الراوتر على الـ لينك

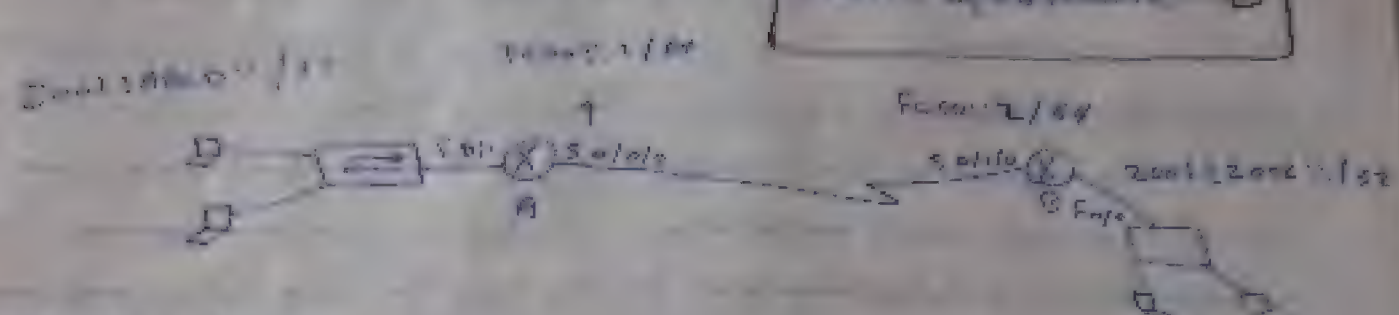
③ FF02 :: 5 → تستخدم ببروتوكول OSPF

④ FF02 :: 6 → تستخدم لـ OSPF لـ DR

⑤ FF02 :: A → تستخدم ببروتوكول EIGRP

## IPv6 Routing Configuration

# Static IPv6 Route ①



## ① Router A

Router > en

Router # Config +

Router(Config) # int serial 0/0/0

Router(Config-if) # IPv6 address FC00::1/64

Router(Config-if) # No shutdown

Router(Config-if) # int Fa0/1

Router(Config-if) # IPv6 address 2001:2002::1/32

Router(Config-if) # No shutdown

Static Route تعريف الشبكة التي ستصل بها

Router(Config) # IPv6 Route 2001:2002::/32 50/0/0

Router(Config) # IPv6 Route 2001:2002::/32 FC00::1/64 أو

Router(Config) # IPv6 Route 2001:2002::/32 FC00::2/64 أو

## ② Router B

نظم الاسترجاع الخاص به كما فعلنا في راوتر A

Static Route التي ستصل بها

Router(Config) # IPv6 Route 2001:2002::/32 50/1/0

Router(Config) # IPv6 Route 2001:2002::/32 FC00::2/64 أو

Router(Config) # IPv6 Route 2001:2002::/32 FC00::1/64

Router # Show IPv6 Route Static



சென்னை நகராட்சி நிர்வாகப் பேரவை உத்தரவு எண் 100/1984  
சென்னை நகராட்சி நிர்வாகப் பேரவை உத்தரவு எண் 100/1984

Defunct? ☐

Quelques A

Router (Config) # Ip v6 Route N/A / 0 Serial o/o/o

Question 3

Router(Config) # IPv6 Router 1. / 0 Serial 0/1/0

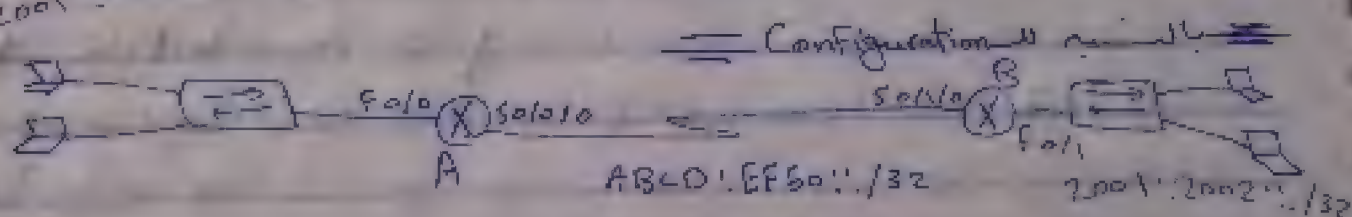
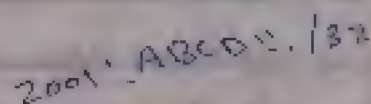
ospf v3 [3]

ospfv3 هو الامتداد الجديد لبروتوكول ospf الذي يعمل مع Ipv6 وانا ان شاء الله

229.0.0.6 عنوان كنوان DR/BDP 229.0.0.5 عنوان كنوان

للمulticast ناه  $ospf v3$  مـ  $FF02::6$  كـ  $DR/BDR$  مـ

العنوان FF02::5 إلى multicast



Router A

Router (config) # If v6 unicast-Routing

Router(Config)# ipv6 router ospf 40 ----- process id

Router(config-rtr) # Router.id 1.1.1.1 ←  $\text{Ip router id}$

```
Router(config-rtr) # exit
```

```
Router(config)# int 50/0/0
```

منه في المصنف لا انتم في المصنف

Router(config-if)# IPv6 OSPF area 0

2014

Area 21

Router(Config) # int F0/0

Router(config-if)# IPv6 ospf 40 area 0

Router B

Router(Config)# IPv6 unicast-routing

Router(Config)# IPv6 Router ospf 50

Router(Config-rtr)# ~~Router~~ Router-id 2.2.2.2

Router(Config-rtr)# exit

Router(Config)# int S0/0/0

Router(Config-if)# IPv6 ospf 50 area 0

Router(Config)# int F0/0

Router(Config-if)# IPv6 ospf 50 area 0

## Show IPv6 Route - ## Show ipv6 ospf

## Show ipv6 protocols - ## Show IPv6 ospf interface

## Show ipv6 interface brief - ## Show ipv6 ospf neighbor

## Show ipv6 ospf database - ## Show IPv6 Route ospf

passive-interface #

في حالة إذا كنت تريد أن تكون الـ interface الـ IPv6 passive-interface الـ IPv6 network

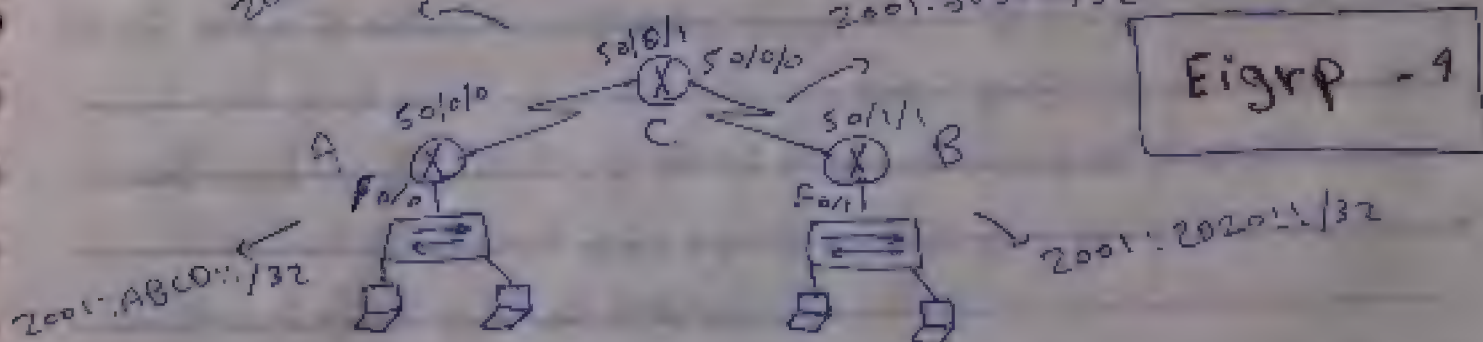
Router(Config)# IPv6 Router ospf 50

Router(Config-rtr)# passive-interface F0/0

# نحتاج تفعيل الـ IPv6 في الـ interface

2001:DB8::/32

2001:5060::/32





Router A

Router(config)# ipv6 unicast-routing

Router(config)# ipv6 router eigrp 5

Router(config)# no shutdown

Router(config-rt)# router-id 1.1.1.1

Router(config-rt)# exit

Router(config)# int Fa0/0

Router(config-if)# ipv6 eigrp 5

Router(config-if)# int S0/0/0

Router(config-if)# ipv6 eigrp 5

وتتبع نفس الخطوات على الراوتر B

وبالآن ننتقل إلى الأوامر

# Show ipv6 eigrp interface

# Show ipv6 protocols

# Show ipv6 eigrp neighbor

# Show ipv6 eigrp Topology

# Show IPv6 Route

# Show ipv6 ~~eigrp~~ route eigrp

## Network management

### NTP II

في الضمان Network time protocol ونموذجي

ضبط الوقت على أجهزة الشبكة بطريقة أوتوماتيكية

حيث تقوم أجهزة الشبكة بحديث الساعة من الوقت والتاريخ

فكره عمله

فكره عمله عبارة عن سيرفر لم ضبط الوقت والتاريخ عليه وتقوم

أجهزة الشبكة بالحصول على الوقت والتاريخ من طرقة الاتصال بهذا

السيرفر مع العلم ان السطع ايضا ضبط الساعة أيضا على الأجهزة بشكل

يسر

II ضبط الساعة يدويًا

Router # clock set 08:05:17 29 mar 2019

نلاحظ أننا كتبنا الأمر على ال privileged وبيانات الساعة في المقام في العنوان

ثم كتبنا التاريخ اليوم في الشهر في السنة

III ضبط سيرفر NTP

\* السيرفر سيكون مفعّل عليه الوقت والتاريخ المراد نقله لكل أجهزة الشبكة

\* نقوم بإعطاء السيرفر IP وهو الذي سنخبره الأجهزة التي ستحصل على

الوقت والتاريخ من السيرفر أنه هو السيرفر

Router > en

Router # Config +

Router (Config) # NTP server { server IP }

Router # show ntp status

Router # show ntp associations.

\* يساعد برنامج NTP في إدارة ومراقبة الشبكة



DNS هي اختصار لـ Domain name system وهي خدمة أو بروتوكول يعمل بتحويل وترجمة أسماء المواقع إلى أرقام.

من الميسر يجب أن نعلم أن أسماء المواقع مثل yahoo.com و google.com وغيرها من المواقع هي في الحقيقة أسماء وهمية وليست لتسهيل التصفح بل تقدم هذه الأسماء وهو من الأساس عنوان IP.

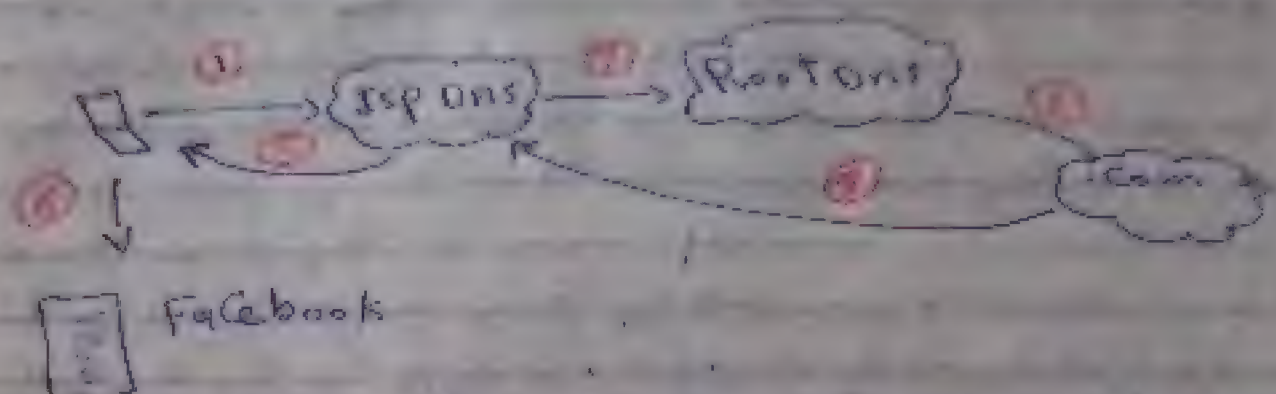
مثلاً موقع google.com عنوانه ال IP الخاص به هو 173.194.35.18 فإذا كتبنا في المتصفح google.com أمراً 173.194.35.18 فإنه النتيجة النهائية واحدة وهي موقع google.com. لذلك إذا كتبنا الاسم فإنه يتحول ال DNS يقوم بترجمة هذا الاسم إلى عنوان IP.

**فائدته** مائة DNS كبيرة جداً حيث لا يستطيع المتصفح حفظ عنوان ال IP الخاص بكل موقع فلهذا فإنه يجب عليه حفظ اسم الموقع وتقوم بروتوكول ال DNS بتحويل هذا الاسم إلى عنوان IP.

**تفكره على**

يقوم المستخدم [Client] بمحاولة الاتصال بموقع ولكنه مثلاً Facebook.com أول مرة يصل فيه يكون الجهاز [Client] لا يعرف ما هو ال IP الخاص بـ Facebook وبالتالي يتصل بـ DNS سيرفر الذي تقدمه شركة ISP المزودة لخدمة الإنترنت الذي يقوم بترجمة الاسم لعنوان IP ويرد ال Client بالعنوان فيقوم ال Client بالاتصال بموقع Facebook. وبخلافه DNS سيرفر الذي عند ISP لا يوجد عليه IP عنوان موقع معين فإنه ال DNS سيرفر الخاص بـ ISP يتصل بـ DNS Root وهو عبارة عن سيرفرات سجل عليها جميع مواقع الإنترنت مثل .com، .net، .org، .edu. وهكذا فيعرف DNS Root عن طريق الاسم المرسل إليه كل عنوان موقع يقع .com، أو .net وهكذا وبالتالي لو .com، يحول الاستفسار إلى سيرفر ال DNS الخاص بمواقع الشركات .com، والذي يكون سجل عليها أسماء والمواقع.

الآن سنشرح كيف يعمل DNS، والهدف من هذا هو ان نفهم كيف يعمل DNS في الخلفية  
الموجود في شركة موزيلا في واشنطن العاصمة في الولايات المتحدة



\* بالطبع لن يحدث ذلك في كل مرة، بل في المرة الأولى التي يرسلها client الى الموقع، فبعد ذلك  
يحتفظ به في ذاكرته، وإذا لم يكن في ذاكرته، يذهب الى الموقع قبل هذا الوقت، ولهذا قد نراه  
في حالة يتم تصفحه عنده، وكذلك في ISP، وبالتالي لن تتكرر العملية

\* سبقتم DNS أيضاً في الشركات حيث تقوم كل شركة بتسجيل بياناتها  
باسماد الأجهزة أو الـ IP، فلو كان الـ IP هو عنوان الـ manager 1  
الشركة أنه يكون العنوان 192.168.1.10، وهو عنوان المدير، مثلاً manager 1  
مادة يتم تصفحه على سيرفر الـ DNS، فلهذا ما يسجل عملية الاتصال حيث  
أنتي أنتذكر الاسم ويحفظ على تذكر عنوانه IP، الخاص بجهاز المدير  
وهذا.

### ملفات الـ DNS

#### ① Resource Records

هذه بيانات المواقع والبيانات الخاصة بها، وتكون مسجلة على سيرفر

#### ② DNS name server

وهو السيرفر DNS، ويكون مسجل على المواقع ما يسجل عليه، وله إمكانية الإجابة  
على استفسارات الـ client، فلهذا يرسل السيرفرات الأخرى لتعلم  
الـ Records التي ليست موجودة لديه

#### ③ DNS Resolver

وهو الخاصية التي يرسلها client الى السيرفرات لتتبع الاستفسار عن الـ Records الغير  
موجود لديه



## SysLog 3

نماذج SysLog و SysLog Message هي قياسية  
لأجهزة الشبكة المختلفة وأيضاً هذه الأجهزة الأخرى  
التي تدعم الشبكة يمكنها إرسال الرسائل التي تظهر عليها أنظمة التشغيل  
عبر الشبكة إلى سيرفرات SysLog ليتم مراجعتها هذه الرسائل ومعرفة ما كان  
وما هو الأوامر التي تم تنفيذها على أجهزة الشبكة سواء أروتر أو سويتش

مثال

عندما نكتب الأمر على الترميز يجعلها down فإنا ندخل على الترميز ونكتب  
الأمر shutdown - تظهر لنا رسالة

E o/o changed state to down

أثناء تغيير حالة الترميز من up إلى down سيتم إرسال هذه الرسالة إلى  
السيرفر الذي نجهزها سابقاً ليتم حفظ كل تلك الرسائل عليك لتتمكن من مراجعتها  
في أي وقت ستحتاجها

فائدته هذه الخدمة أما البروتوكول فيسمح لنا بالقيام بـ monitoring أو مراقبته  
للتأكد من عدم عرقلة تشغيله من خلال إرسال إحصائيات الراوتر والسويتش  
وما هو الأوامر التي تم تطبيقها على الشبكة. وذلك أيضاً يفيدنا في عملية  
ال Troubleshooting لحل مشاكل الشبكة.

# هذه الرسائل يمكن أيضاً أن تُحفظ داخل ال RAM وتسمى ال logging buffer  
ولكن هذه تقطع في حال إيقاف تشغيل الراوتر أو السويتش.

## # شكل الرسالة

# Dec 18 17:10:15.079 : o/o lineproto - 5 - updown : Line protocol  
on interface FastEthernet o/o, changed state to down

تقسم هذه الرسالة إلى عدة أجزاء

- ① الوقت ← Dec 18 17:10:15.079
- ② المزمع الذي ولد أماننا الرسالة ← o/o lineproto
- ③ مستوى الخطورة [The severity level] ← 5
- ④ كذا كبر الرسالة ← updown
- ⑤ وصف الرسالة ← line protocol on interface

Severity level  
 هذه مستويات الخطورة بالترتيب من الأقل إلى الأعلى  
 من الأقل إلى الأعلى

level	level name	
0	Emergency	قد يكون النظام غير قابل للاستخدام
1	Alert	قد يكون هناك حاجة لإجراءات فورية
2	Critical	وقوع أخطاء خطيرة
3	Error	رسالة خطأ
4	Warning	حالة قد تحتاج إلى اهتمام
5	Notification	رسالة تنبيه لأمر ما
6	Informational	إعلام بأمر طبيعي
7	Debugging	الأمور عابرة، قد تأتي من أجل تصحيح خطأ ما

• يجب أن تكون الأوامر موجهة إلى سيرفرات الراوتر أو أجهزة الشبكة  
 إلى سيرفرات الـ Syslog - حواريات أو أجهزة

### تعيين الأوامر الـ Syslog

① قبل عملنا كما فعلنا مع سيرفرات الـ Syslog، نحتاج إلى إرسال هذه الرسائل عليه، وبذلك نكون قد  
 أنهينا عملنا لجهاز سيرفر الـ Syslog

② برنامج الـ Syslog الموجود على الـ PC يمكنه من قراءة رسائل هذه الرسائل  
 المرسله من الراوتر والسويتش مثل برنامج الـ Kiwi Syslog أو الـ TFTP

③ تفعيل الأوامر الخاصة بـ Syslog على الراوتر أو السويتش المراد مراقبته  
 ما لم عليه من إجراءات



Router>enable

Router># Config t

Router(Config)# logging 192.168.10.1

تتم الأوامر مع إرسال الرسالة إلى العنبر 192.168.10.1

\* قياس التكرار: استقبال الرسالة بطريقة محددة مثل أنه عدد مستويات التكرار

Router(Config)# Logging 192.168.10.1 4

Router(Config)# Logging Trap 4 ( 0 ÷ 4 )

\* أو تحديد نوع واحد فقط من الرسائل ممكنة لهذا يكون عدد طريقة كتابة نوع الرسالة مثل التحذير مثل نكتب warning

Router(Config)# Logging 192.168.10.1

Router(Config)# Logging Trap warning

### Modifying system Messages

التعديل على الرسائل يسمح لنا أنه أصل الرسائل بحيث تظهر لنا بأكثر من شكل بدلاً من الظهور بطريقة مؤرخة ولتفعيل ذلك نتبع الآتي

Router(Config)# No Service timestamps.

Router(Config)# Service Sequence-numbers

وبذلك التاريخ أفضل من عملية المراقبة حيث نستطيع معرفة تاريخ الأوامر وهذا تكون المراقبة أفضل ولا رجوع التاريخ فكل ما سبقه

Router(Config)# No Service Sequence-numbers

Router(Config)# Service Timestamps.

أمر ال Show

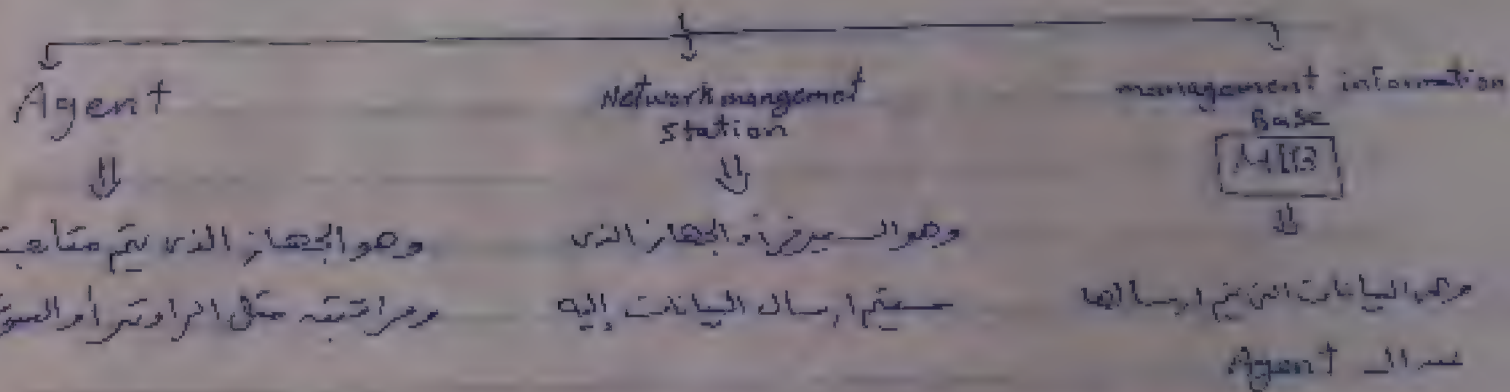
Router># Show logging

# SNMP - 1

هو بروتوكول إدارة الشبكات بسيط Simple network Management protocol  
 يسمح لمراقبة الشبكة من سطح الإدارة مع جميع مكونات الشبكة من أجهزة الشبكة  
 ومطابع وقطع الشبكة لمراقبة أداء الشبكة واستغلال الذاكرة  
 استغلال CPU البرمجيات ومراقبة عمل الجهاز - ومعرفة الحالة العامة  
 ومعرفة حالة الشبكة وإرسال تنبيهات - Traffic على HTTP أو HTTPS  
 أو FTP أو بروتوكولات أخرى

## Snmp Components

يتكون الـ Snmp من ثلاثة أشياء:

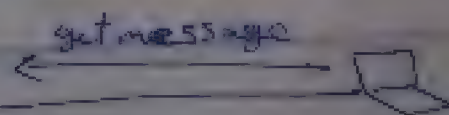


## Snmp message

تنقسم رسائل بروتوكول Snmp إلى ثلاثة أنواع

① رسائل get ← هي الأكثر استخداماً وتنقسم إلى get message  
 و get response

• عندما يرسل السيرفر الـ Agent أنه يرسل إليه البيانات يرسل له  
 رسائل get message



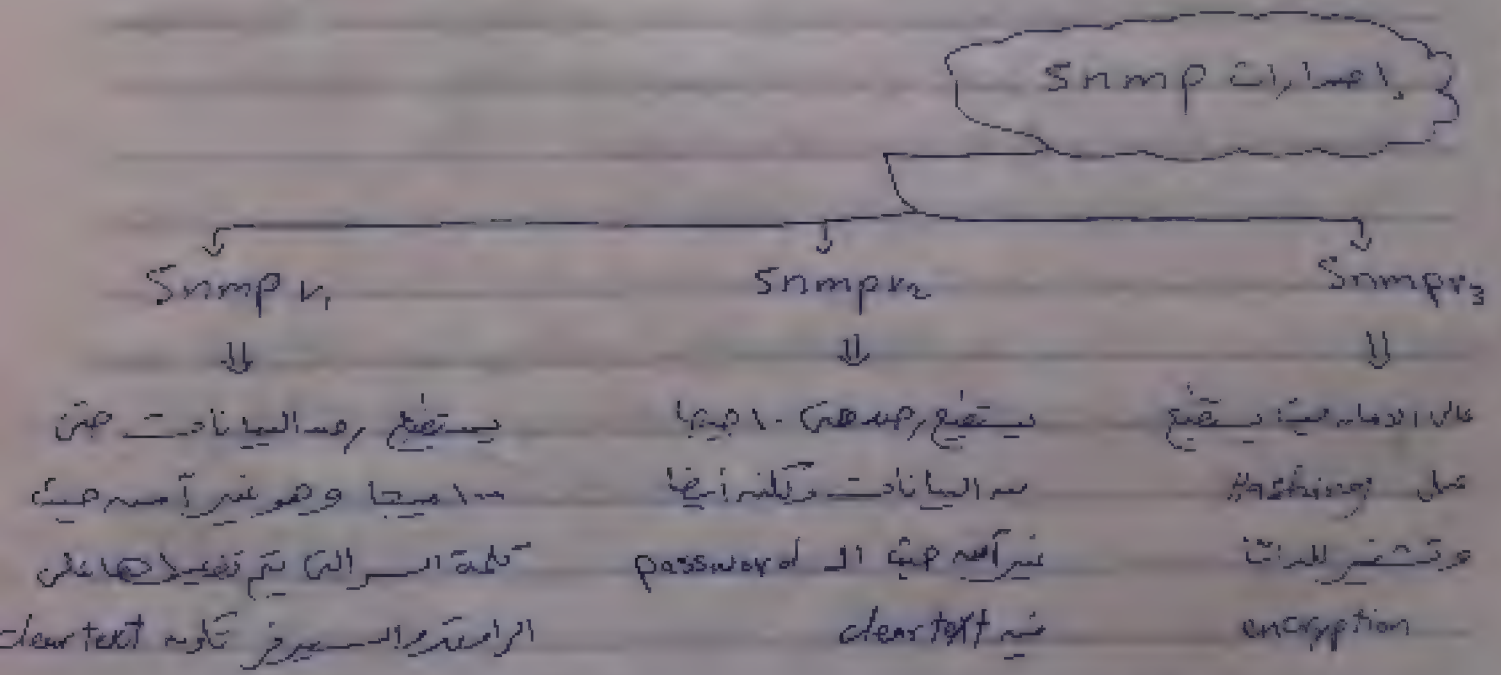
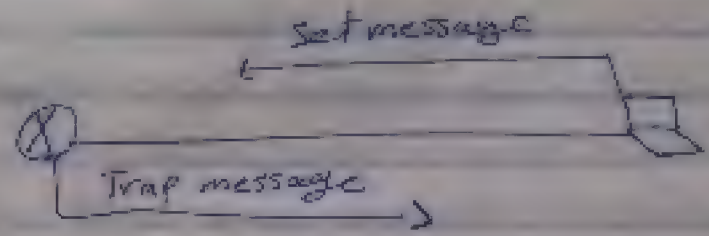


response هو الرد على الطلب الذي يرسله السير  
 message الرسالة

⑧

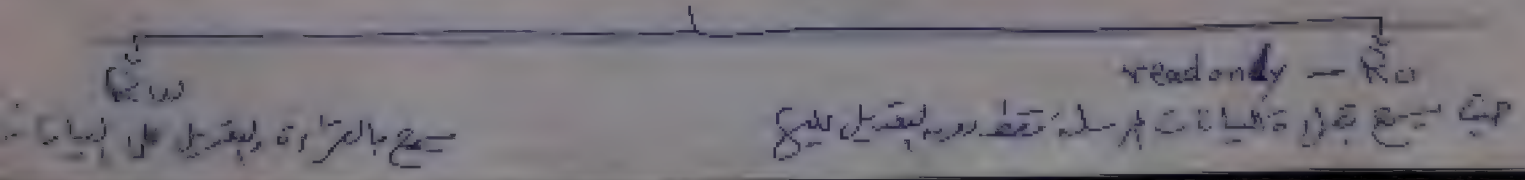
① رسالة Set هي رسالة آخر من رسائل snmp وهي الرسالة التي يرسلها السير إلى Agent بأمره بيفعل الاداة وهذا النوع من الرسائل نادر الاستخدام. وهي الرسالة التي يرسلها السير إذا حدثت مشكلة في السير.

② رسالة Trap هي رسالة آخر من الرسائل يرسلها Agent للسير كتنبيه عند حدوث الشئ الذي لا يفيده شيئاً



snmp v2

بالنسبة لهذا الامتداد فإنه يوفر نوعاً من الاتصال



هذا هو سنمب v2 Read Only  
 Read only

# Snmp v2

الاعتمادية: لا يمكن تغيير البيانات  
 مستوى 1: لا يمكن تغيير البيانات  
 مستوى 2: لا يمكن تغيير البيانات  
 مستوى 3: لا يمكن تغيير البيانات  
 Authentication  
 Data integrity

## Snmp v2 Configurations

Readwrite و Readonly  
 Router(Config) # ip access-list standard  
 Router(Config) # permit host 10.10.10.10  
 Router(Config-std-nacl) exit

Mala Madrid

Router(Config) # Snmp-server Community ...  
 RC  
 RW  
 Read Only

قد يكون من المفيد

Router(Config) # Snmp-server enable Traps ?  
 Router(Config) # Snmp-server enable Traps snmp traps



و بعض الادامر الافتياريه مثل مكانه السيرفر و الاعداد حاله حول سيرفراته  
و بعض التفاصيل

Router (config) # snmp-server contact Ahmed Hobi - network admin

Router (config) # snmp-server location \_\_\_\_\_ في عنوانه مكانه

و هكذا

## NetFlow 5

تقوم برصد كل شيء في Snmp و وظيفته مراقبه الشبكة و الادامه من خلال قليل  
التراميل و مراقبه العاده و ليست من الشبكة و لهذا لياك من ارتفاع اداء الشبكة و هذا البروتوكول  
ليس حصري على اجهزة - يستعمل فقط مكانه مرسومه من شركات اخرى تكلم بسميات مختلفه  
و هذه بعض الامثله

Juniper networks → CFlowd أو JFlowd

Huawei Technology → Netstream For

Alcatel-Lucent → CFlowd For

و غيرها من الشركات

\* و تجلس Snmp بأنه NetFlow يستطيع انه يقدم لنا قليل و متكافئ التراميل من خلال تمهيد  
متكافئ مثلاً ارمه خلال IP معيه و هذا كله يقم به خلال الاعدادات التي نقرم بها  
ما يجب اناه Snmp يقوم بجمع احصاءات أكثر من الجهاز نفسه مثل ال Traffic  
platform و resource utilization و هذا يشمل احصاءات من المبالغ و الرامات و الذاكرة  
التي حست على الجهاز أما ال NetFlow فهو يقوم بجمع معلومات مفصلة حول التراميل  
التي يمر عبر هذا الجهاز

\* يستطيع ال NetFlow جمع معلومات عن

Source IP & Destination IP & Source port & Destination port

IP protocols & interface & IP Type of Service.

\* بعد جمع المعلومات من البروتوكول نعرضها في " Flowcache " في NetFlow Analyzer  
 في NetFlow Analyzer في صفحة " Flowcache " استعراض الترتيب للبيانات

## NetFlow Configuration

① تمهيد البورت الذي - مراقبه وتقبل ال NetFlow

Router(Config) # int f 0/0

Router(Config-if) # ip Route CacheFlow

② تمهيد دخل - مخرج مراقبه ال NetFlow

Router(Config-if) # ip flow egress البيانات الخارجيه

Router(Config-if) # ip flow ingress البيانات الداخله

③ تمهيد الاصدار ال NetFlow

Router(Config) # ip flow-export version 5 او 9

④

④ تمهيد ال Source وال Destination

Router(Config) # ip flow-export source loopback 0

Router(Config) # ip flow-export Destination - الوجه الذي نريد ان يرسل اليه البيانات

⑤ تمهيد وقت حفظ البيانات ال Flowcache

Router(Config) # ip flow-cache timeout active 1

الوقت الذي يتم فيه تحديث البيانات كل دقيقة وطبقا لغيرها حسب اختيارنا

Router(Config) # ip flow-cache timeout inactive 5

الوقت الذي يتم فيه مسح البيانات اذا لم تتسلم البيانات خلال 5 دقائق

أوامر ال Show

Router # Show ip CacheFlow

Show ip ~~Cache~~ cache verbose Flow.



# Managing IOS

أهدافنا اليوم معرفة المكونات الأساسية للـ IOS  
(CPU) وحدة المعالجة المركزية

(RAM) الذاكرة العشوائية تحتوي على الإعدادات العالقة على الراوتر وتنفذ منه البرامج  
بإيقاف التيار الكهربائي

(ROM) تحتوي على برنامج فحص المعلمات الذي يكون في بداية تشغيل الراوتر وتحتوي على  
برنامج Bootstrap المسؤول عن تحميل البرنامج بشكل سليم

(NVRAM) ويحتوي على أنسخة الذاكرة RAM، إذا انقطع التيار عن الراوتر يتم إيقاف التيار الكهربائي  
وتحتوي على الإعدادات المخزنة [الإعدادات بعد التشغيل] وهذا يشبه إعدادات  
الـ RAM، أيها لكن لا تنفذ تلك الإعدادات عند انقطاع التيار الكهربائي

Flash هي ذاكرة دائمة وتستخدم لحفظ وتخزين ملف نظام التشغيل IOS

ports منافذ الـ LAN والـ WAN و Console و Aux

## # خطوات إقلاع الجهاز #

يتم الراوتر بعد مراحل عند عملية تشغيله [إقلاع الراوتر أو التهيئة]

① POST ← هو اختصار power on self test وهي عبارة  
عن عملية فحص داخلي للتأكد من سلامة أجزاء الجهاز [راوتر أو سويتش]  
وهو ما يتم بشكل سليم أو بشكل غير صحيح

[illegible]

في حال عدم توفر الذاكرة في الذاكرة الرئيسية (RAM) يتم تخزين البيانات في الذاكرة المؤقتة (Flash) أو في الذاكرة الدائمة (ROM) أو في الذاكرة الخارجية (Hard Drive) أو في الذاكرة السحابية (Cloud Storage).

\* لمعالجة الإختلاخ نستخدم Bootstrap ملف  $2 \times 2$  وهو الملف الأخير  
أن هو الذي حصلنا عليه من الإختلاخ بصورة عشوائية

• إذا لم يجز Bootstrap ملف، ارفع [IOS] من ذاكرة الفلاش إلى Flash من  
يتم تحميله من IOS في TFTP server

③ المرحلة الثالثة : هي إيجاد دالة تعطيها ملفاً الزمادون المحزنة [ اعداد اعداد السلسلة ]

\* ییجے سے NVRA میں فائدہ پہنچانے کے لیے اقدامات

\* بیجنت ماسکریٹ TFTP server پر قائم ہے۔ یہ سب ایچ ایم ڈی کے ذریعہ

\* یہ خطی متن وضع الاولیاء حضرت ارفاھ علیہ السلام (تکبیر) کا بنی Console

## Router Backup and Restore

## Backup

$$\Sigma = \Sigma$$

مع أجل على نفسه اصطاحه مهل لإعدادات الراوي أدا السوسن

ما خفي في نفسه احتياجه من ملف السجل ١٥٦ فاستأنف تقدم برنامج TFTP  
أدنيوه البرامج تلك TFTP استجابه فاستدرك وهو صغير الحجم  
لقد سجل ١٥٦ من تلك جهاز الكمبيوتر

R# Copy Flash TFTP



هذا الضغط على Enter سيطلب اسم الملف في IP السيرفر وعندها  
نكتب اسم الملف الذي نريد نقله من جهازنا إلى جهاز السيرفر  
السيرفر ونضغط على Enter ثم نكتب اسم الملف الذي نريد نقله من جهازنا إلى جهاز السيرفر

ميكرونو الميكرونو الميكرونو

R# Copy Flash TFTP + enter

لدينا اسم الملف الذي نريد نقله من جهازنا إلى جهاز السيرفر وعندها  
نكتب اسم الملف الذي نريد نقله من جهازنا إلى جهاز السيرفر  
# هذا سيقول الملف الذي نريد نقله من جهازنا إلى جهاز السيرفر

Restored

استعادة الملفات السيرفر TFTP

R# Copy TFTP Flash

سوف نكتب اسم الملف الذي نريد نقله من جهازنا إلى جهاز السيرفر وعندها  
نكتب اسم الملف الذي نريد نقله من جهازنا إلى جهاز السيرفر

Show لإظهار

# Show Flash

# Show version

R# delete Flash - - - bin

Backup Run Start

R# Copy Run TFTP

enter + اسم الملف

R# Copy start TFTP

enter + اسم الملف

هذا سيقول الملف الذي نريد نقله من جهازنا إلى جهاز السيرفر





with the first 1000 cases.

• التباين الجيني هو أساس التنوع البيولوجي، وهو الذي يسمح للكائنات الحية بالتكيف مع بيئتها والتطور.

7.  $\frac{1}{2} \ln \frac{1}{1-x^2} = \frac{1}{2} \ln \frac{1}{1-x} \frac{1}{1+x} = -\frac{1}{2} \ln(1-x) - \frac{1}{2} \ln(1+x)$

مرفقة به الملاحق الى التذكرة رقم 2102 مرفقة بها الى

Decimal	0 1	2	3	4	5
Binary	0 0	0 0 1 0	0 0 0 1	0 0 0 0	0 0 1 0
		1 0 1 0 1 0	1 0 1 0 1	1 0 1 0 1	1 0 1 0

والله اعلم بالصواب

كل Bit له وظيفة ورمزية ال Bit السادس وهو NV RAM  
تدعى علينا صم ال Bit السادس الخاص بـ NV RAM وتلاحظ أنه  
في الملف ال default تحت Binary - نضع 1 إذا جعلنا قيمة البيت  
السادس خاصة ال Binary - جميع الملف التالي


0x 0010 0001 0100 0010

ثلاثة التماسات أصبح واضحا من مرفق مرفق بتحويله من  
Binary إلى التماسات

OX 2 1

4 2  
OX2192 2000

1421

بداية تشغيل الراوتر وإعداد الاتصال مع مودم الهاتف  
نضيف له الزر Ctrl +  common  
وعندها نكتب الأوامر التالية

Router> Config # 2102

بعد ان قمنا بتحميل الملف او تحميله من

Router> reset

بعد الـ router reset نقوم بعملية تثبيت البرنامج  
نقوم به في حال كان البرنامج الـ router بلان لا ماس

Router> en

Router # Copy ~~Run Start~~ Start Run

نقوم بنقل الملف الى الـ router وندخل password

Router # Config t

Router (Config) # enable secret AAA

نقوم بترجيع الـ password الى 0x2102

Router (Config) - Register 0x2102

ونضغط على

Router # wr or Copy Run start

بعد ذلك نقوم بعملية Reload لتفعيل التغييرات

Router # Reload

Grase startup Config

1) إذا أردنا ان نرجع الـ router لحالتها الاصلية ونحذف جميع الاعدادات  
فإننا نستخدم الأمر

Router # write erase

ونضغط على OK Confirm

بعد التأكيد نكتب الأمر Reload

Router # reload

بعد ذلك نقوم بعملية الـ router reset  
الـ router reset نقوم به في حال كان البرنامج الـ router بلان لا ماس

الـ router reset نقوم به في حال كان البرنامج الـ router بلان لا ماس  
enter ونضغط على



(8) ملاحظة : عند حذف VLAN من switch يجب كتابة `delete vlan` لا `erase`

Switch -# `delete vlan dat` → ملاحظة : عند حذف VLAN من switch يجب كتابة `delete vlan` لا `erase`

Switch -# `Reload` ملاحظة : عند إعادة تحميل switch يجب كتابة `reload` لا `reboot`

ملاحظة : عند إعادة تحميل switch يجب كتابة `reload` لا `reboot`

Router  
Switch  
# `erase start`

## أسئلة واجابات العائلات الشخصية

### بعض البروتوكولات العامة

#### ① SMTP

هو اختصار Simple mail Transfer protocol وهو بروتوكول

يستخدم في النقل مع البريد الإلكتروني على شبكة الإنترنت وهو البروتوكول المسئول عن تسليم الرسائل وتوجيهها إلى المستقبل المحدد مسبقاً وهو بروتوكول يعمل ويستخدم البورت (٢٥) وهو بروتوكول (TCP) ويعمل على الطبقة السابعة Application layer

#### ② POP

هو اختصار post office protocol وهو بروتوكول يستخدم مع

البريد الإلكتروني وهو المسئول عن طلب فتح الرسائل أو حذفها أو حفظها وهو المسئول أيضاً عن تسليم الرسائل ولكنه ينفذ وظيفة منه خلال برنامج بسيط مثل outlook أما هذا البروتوكول يسمح للمستخدم بتحميل جميع الرسائل إلى جهازه ومنه ثم قرائتها مع إمكانية حذفها من الجهاز (server) وهو ما لا تستخدمه في الاتصال الضعيف بالإنترنت أو المقطع أو ذو التكلفة العالية لأنه يمكنه من تصفح الرسائل في حالة عدم الاتصال بالإنترنت وهذا البروتوكول له أكثر استخداماً وله إصدارات مختلفة POP<sub>1</sub> ويستخدم البورت (١١٠) والإصدار الثاني POP<sub>2</sub> ويستخدم البورت (١٠٩) والإصدار الثالث POP<sub>3</sub> ويستخدم البورت (١١٠) وهو بروتوكول يعمل في الطبقة السابعة App-layer ويستخدم بروتوكول (TCP)

#### ③ IMAP

هو اختصار Internet message Access protocols وهو البروتوكول

المسئول عن الوصول إلى email server وقراءة الرسائل وهو يعمل على الطبقة السابعة App. Layer وهو المسئول عن طلب فتح الرسائل أو حذفها أو حفظها على السيرفر الخاص بالبريد الإلكتروني انما يملك وله أربع إصدارات تستخدم منه الأخير منها وهو يستخدم uidl بروتوكول والمنفذ (١٤٣)



هذه ظهرت بعد انشاء شبكة من البروتوكولات السابقة والتي تولد ما يسمى بالبروتوكول  
كله تقوم بعملية تشفير للبيانات لحماية البريد من هجمات القرصنة والتجسس  
ورصد

Secure pop<sub>3</sub> (SSL pop) → port [995]

IMAP over SSL (IAMS) → port [993]

Secure SMTP (ssmtp) → port [465]

④ SSL هو اختصار Secure Socket Layer وهو بروتوكول مسئول عن تشفير البيانات  
المتنقلة من وإلى متصفح الانترنت والسيرفر ويقوم بإستخدام هذه  
العملية بطريقة متعاضدية [public key] والآخر [private key]  
ويستخدم هذا البروتوكول لتشفير البيانات الحساسة مثل كلمات المرور واسم  
المستخدم و password اثناء بطاقة الائتمان لذلك يستخدم من مواقع Facebook  
Twitter وغيرها. وهو بروتوكول [TCP] ويستخدم البورت [443]

س. ما هو الفرق بين HTTP و HTTPS ؟

① HTTP هو اختصار Hyper text transfer protocol وهو البروتوكول الرئيس  
المسؤول عن نقل البيانات بين المتصفح و سيرفرات الانترنت وهو البروتوكول  
الانترنت استداما كله البيانات تنقل بطريقة غير مشفرة أي انه يفتقر للحماية وهو بروتوكول  
[TCP] يستخدم المنفذ [80]

② HTTPS هو عبارة عن اختصار Hyper text transfer protocol secure وهو  
عبارة عن مزيج بين بروتوكول HTTP وبروتوكول SSL وظيفته هو تأمين  
قناة اتصال وآمنه بين المتصفح وسيرفرات الانترنت أي انه يوفر الأمان والحماية  
التي افتقدها HTTP لذلك يستخدم في المواقع مثل Facebook و Twitter  
وهو بروتوكول TCP يستخدم البورت [443]



من ماله فائدة وجود سبع طبقات من الشبكات ؟  
\* توفير معظم مصفاتي أجهزة الشبكات تحت منظومة واحدة وفياسية  
\* تقسيم الاتصال بين الشبكة إلى أجزاء أصغر وأبسط مما يسهلها  
من حيث تتبع المشاكل وبالتالي حل المشكلة

من ماله مميزات UDP عن TCP ؟  
\* 1. UDP أسرع من TCP حيث UDP لا يتبع بالموثوقية والتحقق الموجودة في TCP  
ولهذا لا يتطلب اتصال بالاستلام ACK كما أن TCP  
\* 2. استهلاك UDP لقدرة المعالج أقل من TCP

من ماله الغرض منه DHCP و DNS ؟  
DHCP مسؤول عن توزيع الايبيات للأجهزة بشكل آلي  
DNS مسؤول عن ترجمة الأسماء والمواقع إلى ايبيات ثابتة ومحددة  
على سيررات DNS

من ماله الغرض منه FTP و TFTP ؟  
FTP هو بروتوكول File transfer protocol وهو المسؤول عن نقل الملفات  
بين الأجهزة التي تدعم هذه التقنية وهو بروتوكول [TCP] ويستخدم منفذيه  
المتقدي [20] لنقل البيانات والمنفذ [21] مسؤول عن نقل الاوامر Control Connection

TFTP ← نسخة صغيرة من FTP تستخدم لتثبيت أنظمة التشغيل وهو  
أبسط Trivial File Transfer protocol وهو بروتوكول [UDP] ويستخدم  
المنفذ [69] ولونه UDP فانه أسرع من FTP حيث الأخير TCP

من لماذا عليك FTP منفذان 20 و 21 ؟  
المنفذ [20] هو المسؤول عن نقل البيانات بين العميل والخادم  
Data Connection بينما المنفذ [21] مسؤول عن نقل الاوامر  
Control Connection



من ماله خطوات العودة كلمة السر على روترات سيسكو ؟

1 \* الاتصال من خلال ال port console

2 \* تخطي ايمجاز وابتداء الاتصال وعند ظهور علامة > اكتب ## ## ## ##

3 \* Break + Ctrl للعودة وضع ال Rommon

4 \* تغيير ال Registerfile الى 0x2102 بدلاً من 0x2102

5 \* Reload للراوتر ونظف الذاكرة ونشغل الذاكرة لل Run

6 \* Copy Start Run

7 \* نقل الذاكرة

8 \* نرجع الملف 0x2102 من الذاكرة Router(config) # register 0x2102

9 \* Copy Run Start

10 \* Reload Reload

11 \* Reload